CAL POLY
California Cybersecurity Institute

Windows and Android Forensics
CCIC Training
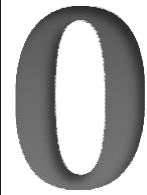## Chapter 0: Preamble

Cassidy Elwell and James Poirier

March 2020 (Version 3)

0

Preparing for the CCIC 2020

The 2020 California Cyber Innovation Challenge (CCIC) will be hosted by the California Cybersecurity Institute (CCI). Training is provided for the DFC at https://cci.calpoly.edu/events/ccic/2019-df-downloads.

As part of the DFC, teams will be presented with a case where digital AND physical evidence will have to be collected, verified, analyzed, and a criminal case will have to be assembled on a timeline and presented to a judge. Digital forensics, critical thinking, teamwork and communication skills will all be tested as part of this event.

In preparation of the DFC, it is highly recommended that the DFC training is completed by all team members. The Windows and Android Forensics CCIC Trainings are designed to take an inexperienced high school student about 22-27 hours to complete. However, the trainings can be split amongst team members to be specialized within areas of Windows and Android Forensics resulting in about 6-8 hours per student.

The DFC training serves as a primer - which covers the necessary skills for teams to compete in the challenge. However, there will be portions of the DFC that will NOT be covered by the DFC training, and your team's ability to handle these unexpected challenges will be a part of your team's overall success.

What is Digital Forensics and how will it be used in the CCIC 2020?

Digital Forensics is a subset of the field of forensics science and has evolved out of computer forensics as digital devices now not only include computers, but other digital devices. Nearly all modern day crimes now have a digital element. However, there is a large divide between the number of law enforcement officers with formal training in Digital Forensics and the number of crimes with a digital element. The DFC is designed to highlight some of these challenges and we believe serves as an example of how "human" cyber problems can be.

Digital Forensics can be broken down into multiple stages, which include:

1. Seizure - Focusing on the preservation of evidence to be legally permissible in court
2. Acquisition - Ensuring evidence is forensically sound (authentic and not tampered with)
3. Analysis - Identifying the evidence and establishing a timeline for the crime
4. Reporting - Putting together a concrete case, often for a non-technical audience

Seizure

After an introduction of the DFC on June 24th, teams will be issued a blanket warrant for searching allocated space(s) to search and seize digital evidence. Please refer to the Windows and Android Forensics CCIC Trainings on the proper seizure of evidence

Acquisition

The acquisition stage of the DFC will be aided by "forensics technicians." Teams that seize a piece of digital evidence will be turning these devices to a "forensic technician" in exchange for a USB drive with a forensics image (creating a forensics image may take several hours). Drive hashes should still be verified upon receipt of the forensics image and once again at the end of the Analysis phase. The Windows and Android Forensics CCIC Trainings will help prepare teams in this regard, but the DFC will provide forensics images to all competitors to avoid long imaging durations.

Analysis

Due to the complexity of the field of Digital Forensics, the DFC's evidence will focus mostly on Windows and Android-based forensics and serves as the bulk of the training. Note that there will be some physical evidence and other digital elements as part of the DFC which will require teams to be able to integrate evidence from multiple sources.

Reporting

After the Analysis phase, teams will have to make an oral presentation (aided by a presentation slide deck, if desired) to a series of judge advocates. The report should focus on the "Who, What, Where, When, and How" will/did this crime take place, and provide evidence supporting these findings. Additionally, teams will be asked to provide recommendations for remediation - what should be done at the outcome of their findings.

Open-Source Tools for Trainings

All tools utilized in these training manuals are open-source and therefore available for download through the links provided.

Prior to starting the trainings, you will want to install/have access to the following tools on your PC:

Windows Forensics

1. Autopsy and/or Sleuthkit
2. Registry Explorer
3. Ophcrack v 3.7 and Vista Free Table
4. Autopsy's Multi Content Viewer 3rd Party Plugin
5. DCode v 4.2
6. JumpLister v 1.1.0
7. USB Historian v 1.3
8. SkypeLogView v 1.55
9. 7Zip v 16.04
10. USB Deview

Android Forensics (Optional This Year)

1. QuickHash GUI
2. Google Map Creation
3. Thunderbird Mail

Additionally, you may want to download the Windows and Android Forensics CCIC Training manuals and training images located at: http://cci.calpoly.edu/ccic.

Note: UFED Reader is a free program provided with the creation of an extraction report and therefore is not an executable which can be downloaded online.

Recommended Training Schedule

It is recommended that all team members complete all training materials. The following is a recommended training schedule, assuming that team training session are each about 1-2 hours long:

Windows Forensics

- Chapters 1-4 – Introduction, Starting a Case, Drive Geometry, Image Verification, Registry
- Chapter 5 – Windows File Overview
- Chapter 6 – Recent Files
- Chapters 7-8 – Recycle Bin, External Storage Devices
- Chapter 9 – Email
- Chapters 10-11 – Internet History, Chat Logs
- Chapter 12 – Hidden Data
- Chapter 13 – Installed Programs
- Chapter 14 – Legality, Reporting
- Appendices, as time allows

Android Forensics

- Chapters 1-3 – Introduction, Secure the Device, Data Extraction with UFED
- Chapters 4-6 – Image Verification, UFED Reader Basics, Lock/Home Screens, Personal Files
- Chapters 7-9 –Installed Applications, Contacts, Phone, Messaging, Location Data
- Chapter 10-11 – Calendar, To-do Lists, Notes, Email, Internet History
- Appendices, as time allows

Note: Android Forensics Chapter 3 on Data Extraction with UFED is for your team's knowledge of understanding the mobile forensics process. You will exchange any mobile phone(s) for a USB drive containing a physical data extraction during the competition.

The training manuals will be available to all teams during the competition, but familiarity with the topics in the training manuals will greatly impact your team's performance. It is therefore also recommended immediately prior to the CCIC that individual team members are assigned to "own and review" one or more of Chapters 6-14 of Windows Forensics and Chapters 4-11 of Android Forensics.

Questions

If you have any questions about the CCIC, or the CCI in general, please do not hesitate to email us at cci@calpoly.edu.

Cal Poly
California Cybersecurity Institute

Windows Forensics CCIC Training
Chapter 1: Introduction

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

1

Introduction

During this CCIC Event, there will be a computer forensics challenge where you will have to analyze digital evidence. The documentation provided will help ease you into how to conduct analysis on digital evidence and how to triage a case. You will be provided evidence files with specific case scenarios to work through. The first evidence file this documentation will walk you through is the Craig Tucker case. The following is the scenario for the Craig Tucker case:

Tucker Case Summary

As part of a normal business practice, Walmart security receives Counterfeit Coupon Alerts from the Coupon Information Corporation. Within the past month, Walmart security has received specific information regarding fraudulent coupons being passed at their store. Using the information they received, they conducted an internal investigation using video surveillance footage in an effort to identify the customers who are engaged in this activity.

One of the suspects was an unknown white, male adult, approximately 28 years old, brown hair, 5' 9", 200 pounds, no facial hair, and no visible tattoos. A photograph of this suspect was circulated to the employees in the store.

On December 22, 2013, Craig Tucker was detained by Walmart security as he matched the description and he had just passed 2 fraudulent coupons for Monster energy drink and Arizona Ice Tea beverages while paying for other items.

Walmart security contacted the Santa Monica Police Department to arrest and prosecute Tucker for theft.

Santa Monica PD Officer Smith interviewed Tucker and he denied knowing the coupons were fraudulent. He claimed to have received the coupons after completing an online survey for students at Santa Monica Community College.

Although Tucker gave consent to the search of his personal computer, a search warrant was obtained to search his computer for evidence as it may be an instrument to committing a crime.

You have been given a forensic image of his hard drive. Based on your review of the search warrant, you are authorized to search for any information or communication associated with the creation, downloading, distribution, and possession of fraudulent consumer coupons.

Craig was caught with the following coupons:

After working through the documentation and the Craig Tucker case, you will be given some questions on the evidence and your findings. As you provide your answers, you will be given feedback as to whether or not you had the correct results and where you can look to find the correct results.

Once you complete the Tucker evidence file, you will be provided two additional evidence files you can use for practice. The Kip and Rico cases have their own case scenarios and you will analyze the evidence the same way you did the Tucker evidence. You will also be given questions on your findings for these practice evidence files and feedback based on your answers.

Documentation Phased Approach

This documentation is designed for a new forensic examiner to start the analysis of digital evidence using a phased approach. Often new examiners will start with an "everything and the kitchen sink" method, which will lead to a lot of distractions, frustration, and unproductive use of time. This documentation will walk you through how to conduct an investigation, where evidence can potentially be stored, and it will prepare you for the computer forensics challenge during the actual CCIC event.

The phased approach methodology that this documentation follows is based on years of case triage experience. It is designed to keep your analysis focused at a high level and then drill down into targeted areas as needed.

Phase 1 is about setting up the foundation of your case analysis and is broken down into the following sections:

1) Create your case
2) Verify the forensic image
3) Check the drive geometry
4) Determine the operating system
5) Establish the time zone
6) Identify the computers users

Phase 2 is where you will begin to delve deeper into specific areas and it is made up of the following sections:

1) Look for the user's personal data
2) Examine LNK files and jump lists
3) Inspect the recycle bin
4) Check for external storage devices
5) Review the user's email
6) Examine Internet history
7) Check for chat logs
8) Look for hidden or encrypted data
9) Carve data from unallocated space (if necessary)
10) Determine installed programs
11) Scan for malware

Cal Poly
California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 2: Starting Phase 1

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

2

Starting Phase 1

Introduction

When you are first given a forensic image to conduct analysis on, you need to use forensic software and create a case. For this training, you will use Autopsy and other third-party tools. Creating your case while using forensic software like Autopsy is the very first step, and it involves adding your forensic images, setting the case information, and adjusting the time zone for your case. While you search through the evidence in the software, your work will be saved. This allows you to reopen the case later to look through the evidence again if necessary. Therefore, the following are steps you MUST do if you are doing analysis of a **Windows** system. This training does not cover analysis of other systems.
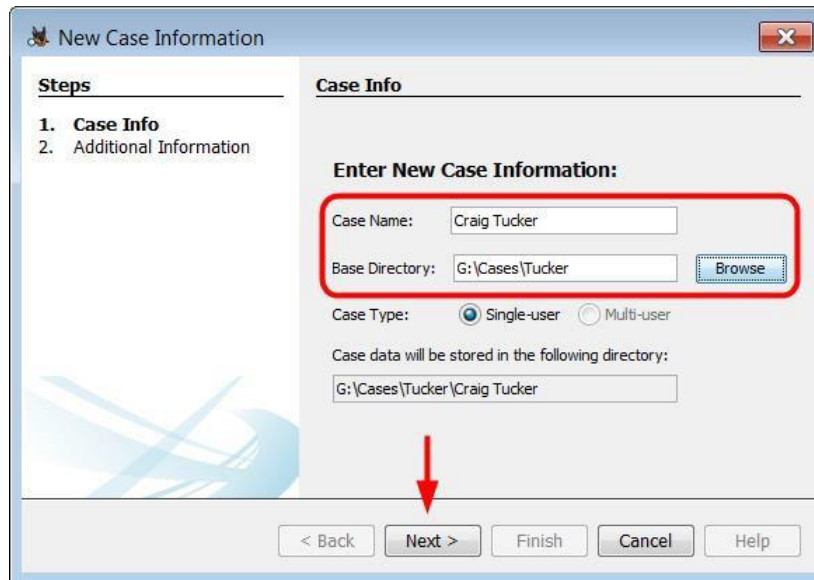
Creating Your Case

This section assumes you have already properly installed Autopsy on your forensic computer. Start Autopsy and click on Create New Case.

Figure 2-1 – Create New Case
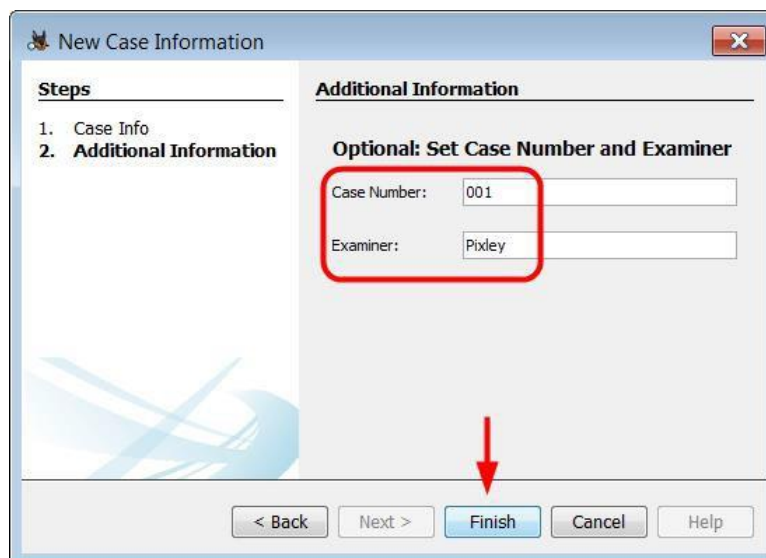
A New Case Information window will open and you need to set the Case Name. Set it to Craig Tucker since that is the first case you are going to work on. Set the Base Directory to where you want your case saved on the computer and then click Next (see Figure 2-2).

Figure 2-2 – Set Case Name and Base Directory

On the next "New Case Information" window, set a case number and your name. Click Finish.

Figure 2-3 – Set Case Number and Name

An Add Data Source window will open and you need to select Disk Image or VM File as the data source type. Click on the Browse button and then navigate to the Tucker.E01 file you have downloaded and click Open. For now, set the time zone to (GMT + 0:00) GMT. We will later cover how to determine the time zone that the computer was set to. Leave "Ignore orphan files in FAT file systems" unchecked and then click Finish (see Figure 2-4).
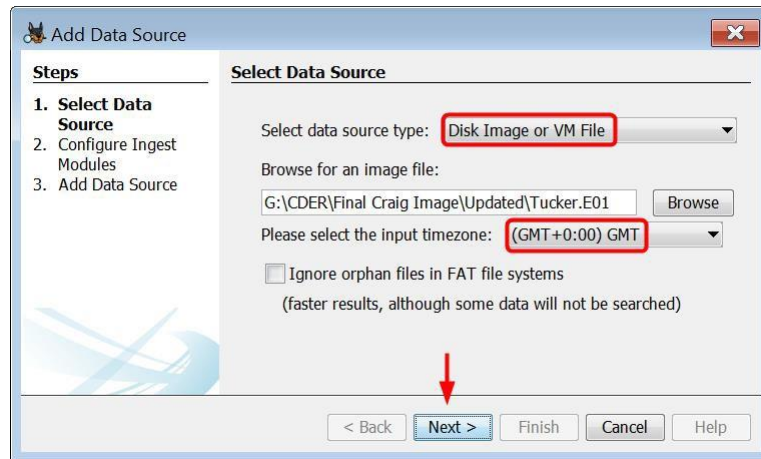
Figure 2-4 – Set Data Source to Disk Image and Navigate to Tucker.E01

On the next Add Data Source window, click the Deselect All button and leave Process Unallocated Space checked. When you are working on a live case, you may not have time to wait for all of these modules to process, and they may not always be helpful with the evidence you are trying to look for. You can always run these modules later during your investigation if necessary as well. Click Next.
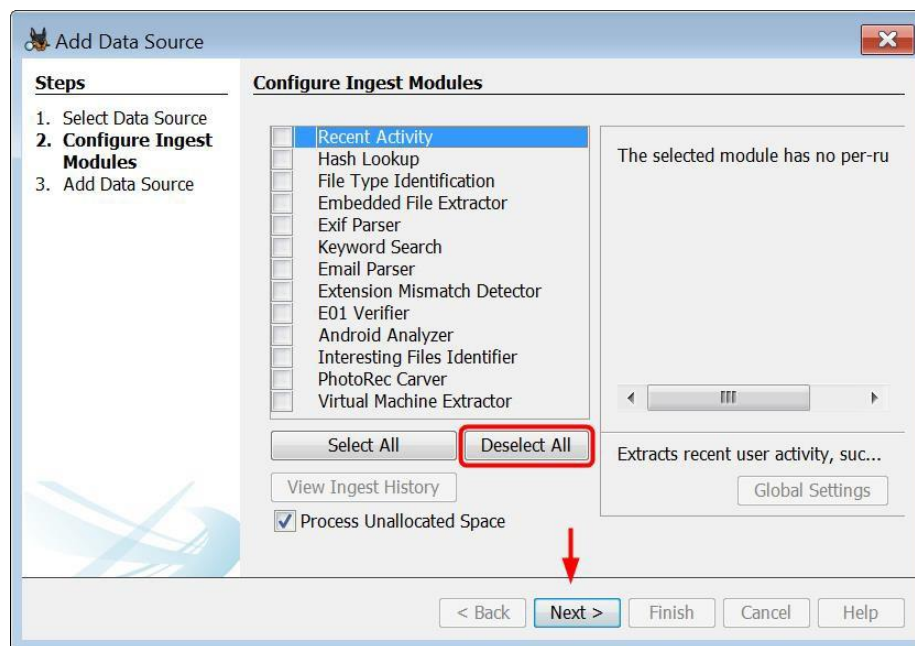
Figure 2-5 – Click Deselect All Button and Click Next

On the last Add Data Source window just click Finish and then wait for Autopsy to finish processing the evidence.

CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 3: Verification

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

3

Verification

Introduction

Before you even begin your analysis, you always want to first establish a solid foundation. You generally want to make sure that the forensic image verifies by checking its hash value. A hash value is basically a fingerprint for a file. The chance of two MD5 hash values being the same is $1/2^{128}$. By checking the hash value of the forensic image and comparing it to the hash value when it was imaged, you are confirming that the evidence has not been corrupted or tampered with. This becomes a vital piece of information later when you are being questioned on the integrity of the image and if you missed any partitions or data. The hash value should be checked once again after investigation is complete to ensure that you haven't unintentionally changed your evidence.

Note: In some simulated images that are created for you, the MD5 hash will not compute. This is due to some technical difficulties in the Virtual Machine that prevent an export with an MD5 computable hash as a .E01 File. This is ok when doing challenges like the CCIC or trainings, but in a real investigation you should always be able to, and should run the MD5 hash verifier. This ensures that your evidence is admissible in court and that the image itself was not tampered with.

Verify the Image

After creating a case and having Autopsy open the evidence, you want to have Autopsy verify the forensic image. To verify the image, you need to run the E01 Verifier module. This was one of the modules that you could have run when you first created the case. However, since you did not run any modules at the beginning, you can always click Tools►Run Ingest Modules►Tucker.E01. This will allow you to run or rerun any of the modules that were available at the beginning (see Figure 3-1).
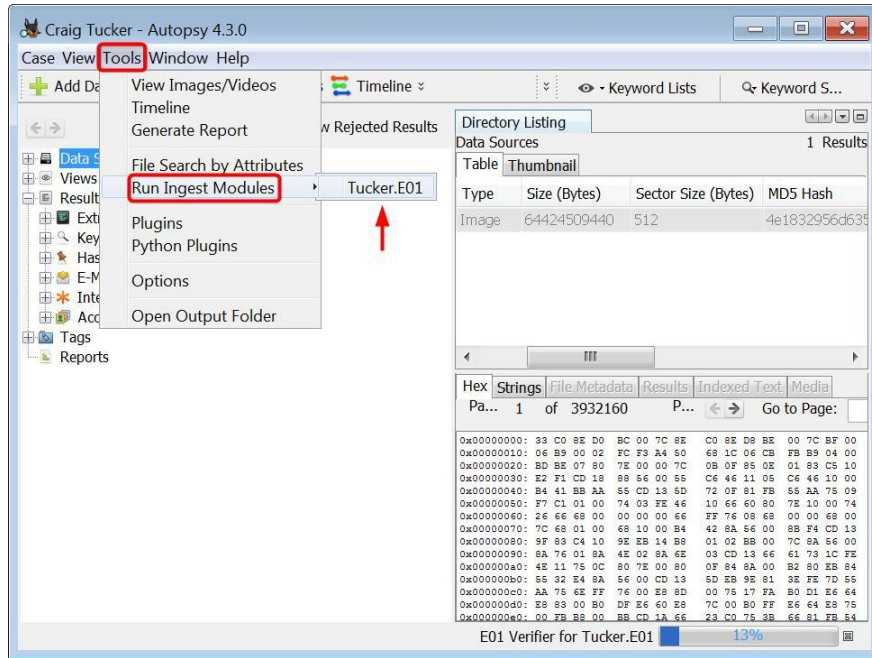
Figure 3-1 – Run Ingest Modules

When the Run Ingest Modules window opens, check the E01 Verifier module and then click Start.
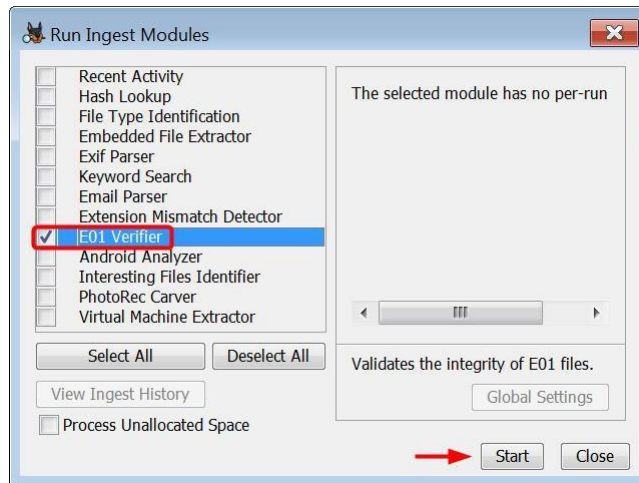
Figure 3-2 – Check E01 Verifier and Click Start

Autopsy will take a few minutes to verify the evidence file. Once it is processed, you can mouse over the drop-down arrow in the top bar and then click on the Ingest Messages button (see Figure 3-3).
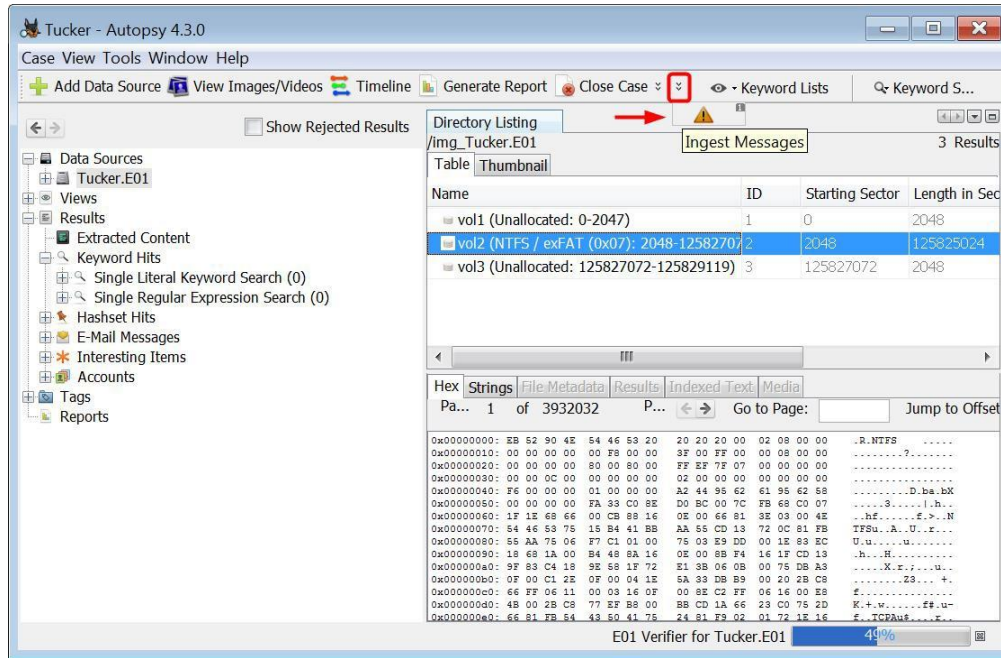
Figure 3-3 – Mouse over Drop-Down Arrow and Click Ingest Messages

There should be two entries in the Module list. One will say Starting Tucker.E01 and the other will say Tucker.E01 Verified. Click on Tucker.E01 verified in the Ingest Messages list, and Autopsy will show you the results that the Tucker.E01 verified and its calculated hash value matches the stored hash value. This means that the forensic image you have is the same and has not been corrupted or changed since it was first imaged.

Figure 3-4 – Tucker.E01 Verified

CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 4: Understanding the Registry

Lauren Pixley, Cassidy Elwell, and James Poirier

4

Understanding the Registry

Introduction

As you are going through your investigation, you will need to know basic information about the forensic image you are searching. To find out more about the image you are analyzing, you will need to look through the Windows Registry. The Windows Registry is basically a database that stores thousands of records with information, such as the operating system, time zone, user settings, user accounts, external storage devices, and some program data.

When you look through the Windows Registry in the next section with REGEDIT, it may appear as though the registry is one large storage location. However, there are several files where the information is being stored throughout the computer. REGEDIT simply takes these files and records stored in different locations and displays them for you. There are many records in the Windows Registry that will have no forensic value to you as an examiner, but there are some pieces of information that you will find useful. This chapter will walk you through the basic structure of the registry and where you need to look to find information that is valuable to your investigation.

REGEDIT

In this section, you will start with the Windows registry utility known as REGEDIT.exe. You can open this by pressing the Windows key+R and then typing in "REGEDIT". You can also click on the Start menu and type "REGEDIT" in the Search box.

Note: REGEDIT.exe displays your computer's registry. You should not make any adjustments to your registry unless you know what the change will do to your computer.

When conducting a forensic examination of a target hard drive, you will not see the same subtrees displayed in REGEDIT. However, most information you come across on the Internet will be notated in a format that assumes you are using REGEDIT. For example, you may find information showing you the location for a user's home page setting for Internet Explorer written as:

```
HKEY_LOCAL_MACHINE\SYSTEM\[CurrentControlSet]\Control\TimeZoneInformation
```

However, if you received information from another examiner, he may have written it as:

```
SYSTEM Hive: [CurrentControlSet]\Control\TimeZoneInformation
```

Both of these locations are exactly the same; it just depends on how you are viewing them.

It is a good idea to start using proper terminology so there is no confusion when you are documenting your findings. The first terms you need to become familiar with are subtree, key, subkey, hive, and value.
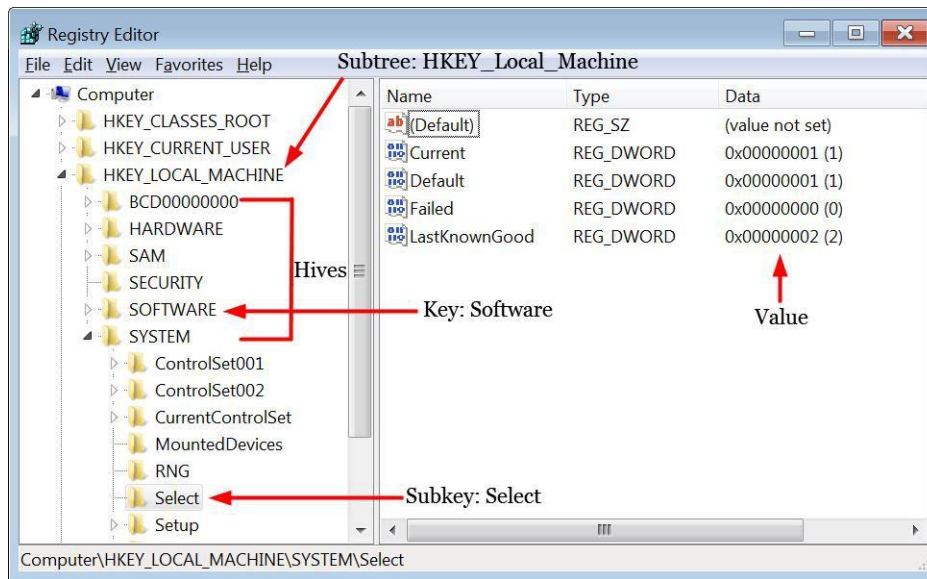
Figure 4-1 – Windows Registry Terms

Subtrees, Keys, and Subkeys

There are 5 *subtrees* that make up the Windows registry. The following list contains each subtree, the standard abbreviation, and the type of information found within each subtree:

Subtree	Abbreviation	Description
HKEY_CLASSES_ROOT	HKCR	Contains information about file extension associations and the Object Linking and Embedding (OLE) database.
HKEY_CURRENT_USER	HKCU	Contains user information, preferences, and settings for the user that is currently logged on (in this case, you will see your settings).
HKEY_LOCAL_MACHINE	HKLM	Contains computer-specific information, such as software, hardware, and security.
HKEY_USERS	HKU	Contains user information from the user currently logged in, the default profile, and system accounts.
HKEY_CURRENT_CONFIG	HKCC	Created during the boot process and contains information associated with the hardware configuration.

Below the HKEY_LOCAL_MACHINE *subtree*, there are five *keys*, which are also called *hives*. Below each *key*, such as SYSTEM, there are *subkeys*, such as Select.

Hives

The Windows registry has several system files called hives, with each hive being mapped to a single file. The HKEY_LOCAL_MACHINE (HKLM) subtree contains settings that apply to the local computer's configuration and affect each user that logs on. There are four main hives that are associated with HKLM, and the list below displays the name of each hive and the actual filename associated with that hive:

Hives	Location of Hives
HKEY_LOCAL_MACHINE\SYSTEM	C:\Windows\system32\config\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE	C:\Windows\system32\config\SOFTWARE
HKEY_LOCAL_MACHINE\SECURITY	C:\Windows\system32\config\SECURITY
HKEY_LOCAL_MACHINE\SAM	C:\Windows\system32\config\SAM

Note: Backups of the hives are located in C:\Windows\system32\config\regback. Look at the Modified dates of those files to determine if they may contain old information that could be useful to your investigation.

With REGEDIT, you will see a key called HARDWARE. However, there is not a system file that matches this key. The key is volatile in memory, so you will not be able to see it during your analysis. It contains information about the hardware devices that were detected during the boot process.

Values

You need to be familiar with the terms *value name*, *value data*, and *value type*. Each subkey in the registry contains at least one or more values. In Figure 4-1, there is a *value name* of LastKnownGood and its *value data* is 2. The registry also contains different types of data, which is referred to as a *value type*. Here is a list of values types:

Value Type	Description
REG_NONE	No defined value type.
REG_SZ	Null-terminated string that will be either ANSI or Unicode.
REG_EXPAND_SZ	Null-terminated string that contains references to environment variables.
REG_BINARY	This is binary data and it's displayed in hexadecimal notation.
REG_DWORD	A 32-bit number. The values stored are sometimes used as Boolean flags (00 = disabled; 01 = enabled).
REG_DWORD_BIG_ENDIAN	This is a double-word value stored as big endian (most significant byte first).
REG_MULTI_SZ	Array of null-terminated strings, terminated by two null characters.
REG_QWORD	A 64-bit number.

As you look at values stored in the registry, remember that an application can store data in different ways and the interpretation is up to the program. Never assume a value means something unless you have confirmed the setting. For example, you may see a value of 0 and assume that means disabled; however, the programmer might have used the value of 0 to mean not disabled (therefore it is enabled).

User Profiles

On Windows 7 and 8 computers, the user profile is stored in a separate folder for each user under C:\Users\[username]. Each user profile folder contains a profile hive, which is a system file called NTUSER.DAT.

When a user is logged in, the user's NTUSER.DAT file is mapped to the following two subtrees:

HKEY_CURRENT_USER

HKEY_USERS

Under the HKEY_USERS subtree, there are some additional profile hives, which are listed below:

HKU\S-1-5-18   Local System (same as .DEFAULT)

HKU\S-1-5-19   LocalService NTUSER.DAT

HKU\S-1-5-20   NetworkService NTUSER.DAT
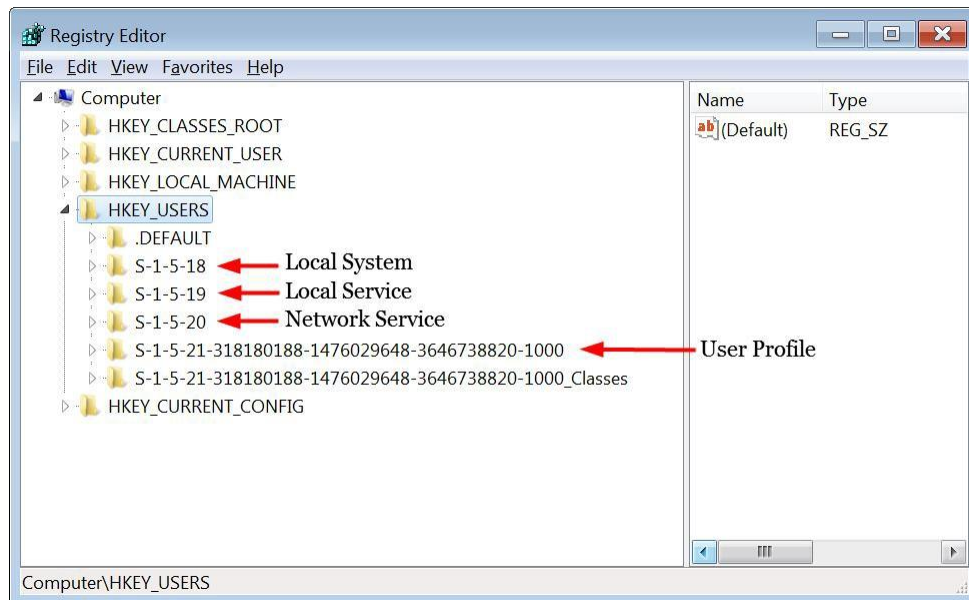
Figure 4-2 – User Profiles in Registry

Security Identifiers (SID)

Under HKEY_USERS, you will see *Security Identifiers* (SID), which is part of Windows security. Windows uses a concept referred to as a *security principle*, which would include items such as computer accounts, user accounts, user groups, and other security-related objects.

On a local computer, the *Local Security Authority* (LSA) generates a SID for local security principles and then stores them in the local security database.

In Figure 4-3, you can see a SID of S-1-5-21-674973493-240844686-639060511-1002, which can be broken down into the following components:

[S]-[*version*]-[*identifier authority*]-[*domain identifier*]-[*relative identifier*]

The first 3 characters of a SID consist of:

S: A SID always begins with S

1: SID version

5: Identifier authority (5 is NT authority)

The following string of numbers (21-674973493-240844686-639060511) is the *domain identifier*.

The last 4 bytes of the SID is a *relative identifier* (RID), which is the account or group. Some of the common RIDs are:

500   Administrator

501   Guest

1000+   User Accounts

Microsoft lists well-known security identifiers on their website:

```
http://support.microsoft.com/kb/q243330
```

Operating System

Now that you have a good understanding of Windows time stamps and the registry, you can check the suspect's operating system. This is an important step before you begin your analysis, because you need to know what type of artifacts you are going to find and where they are located. Where are the user's documents or recent folder located? How is data being stored? If the suspect deleted something, can it be recovered? All of these questions and many others start to become easier to answer once you know what operating system the suspect was using.

The operating system information is stored in the SOFTWARE hive. This is located in:

```
C:\Windows\System32\config
```

Note: This current version of Autopsy (4.3) has issues opening the System32 folder since there is a large amount of data in it.

To view the time zone information stored in the SOFTWARE hive, you need to run another built-in module. Click Tools►Run Ingest Modules►Tucker.E01. When the Run Ingest Modules window opens, check Recent Activity and then click Start.
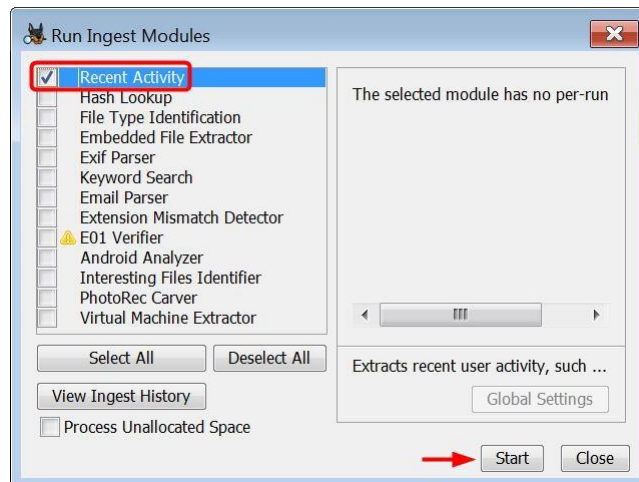
Figure 4-3 – Check Recent Activity Module and Click Start

The Recent Activity module will pull web browser history data and important registry information so you do not have to manually find the data. However, it is still important to know where this information is being pulled from so you could manually find and verify the results if necessary. We will further cover where this data is stored in the registry as we view the results.

Once the Recent Activity module finishes running, you can click on Results►Extracted Content►Operating System Information. The last entry in the table pane shows that the operating system is Windows 8.1 Pro. It also shows that the owner of the computer is simply just Windows User (see Figure 4-4). This information has been extracted from the SOFTWARE hive and is stored under the following subkey:

```
Microsoft\Windows NT\Current Version
```
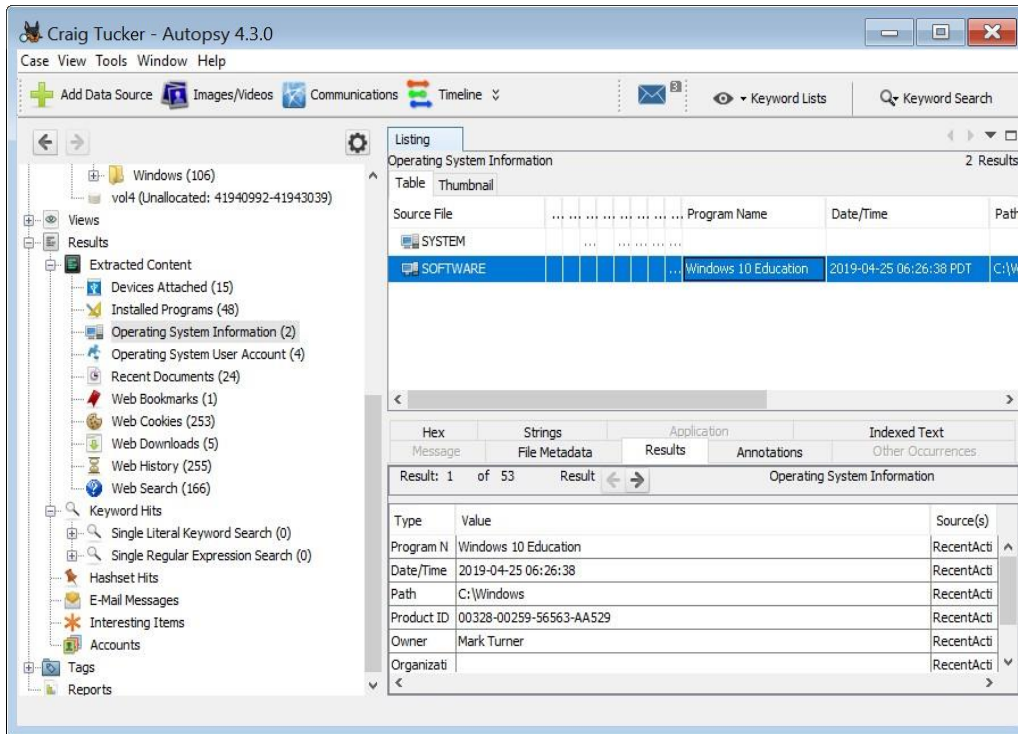
Figure 4-4 – Operating System Information Extracted from SOFTWARE Hive

Note: There is another SOFTWARE entry in the table pane because there are backups for each registry hive.

Registry Explorer

The information that Autopys extracts from the SYSTEM hive is useful, but it is very limited. If you want to further explore the user's registry and find more information, you will need to use another tool. For this case, we are going to use the tool called Registry Explorer. You can download it from:

```
https://ericzimmerman.github.io/
```

To use the tool, you will need to extract the registry hives from Autopsy. First, you need to right-click SOFTWARE in the table pane and select
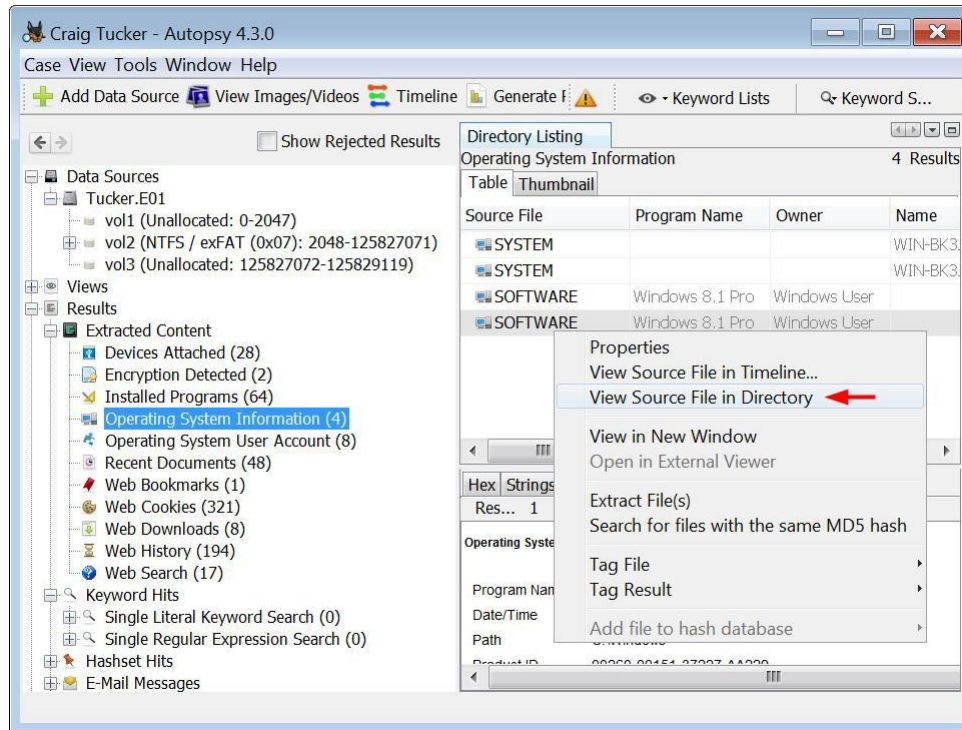
Figure 4-5 – Right-Click SOFTWARE Hive in Table Pane and Select View Source File in Directory

This will take you to the config folder where the registry hives are stored. You will want to export out the SOFTWARE, SYSTEM, and SAM hive from the config folder. To do this, click the first hive then press the Control key while clicking on the other hives. This will highlight all three files. Right-click one of the hives in the table pane and select Extract File(s) (see Figure 4-6).
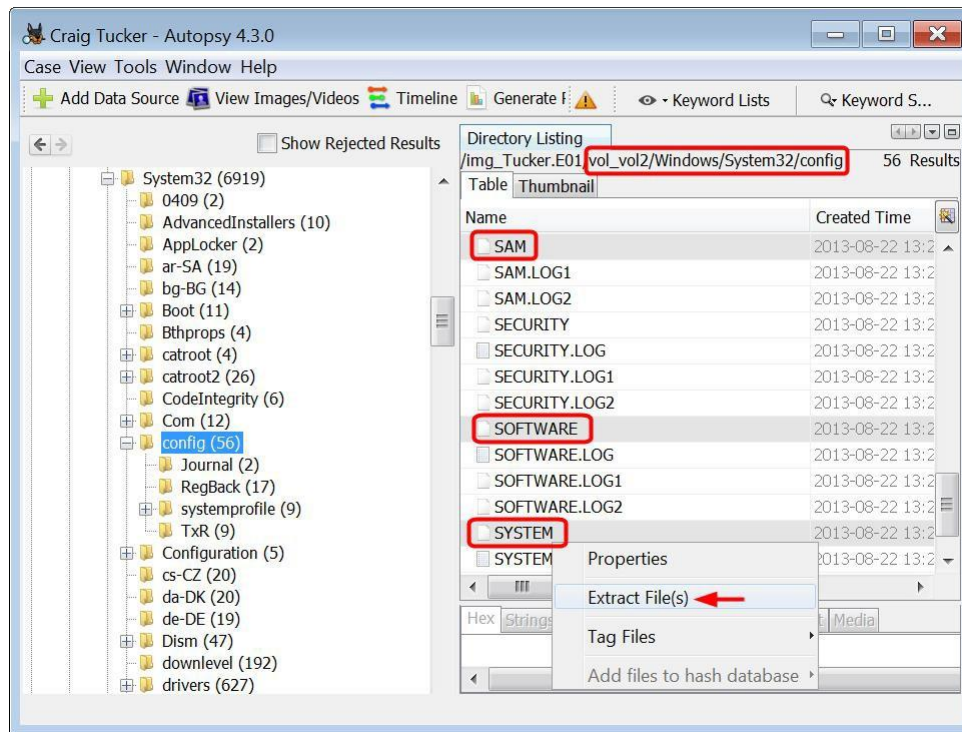
Figure 4-6 – Highlight SAM, SOFTWARE, and SYSTEM, Right-Click One and Select Extract File(s)

A Save window will open, and you need to create a folder to export the registry hives to. Once you have an export folder, click Save.

Note: Sometimes when Autopsy exports these registry hives, they attach a number to the name. Some tools may not recognize or open these renamed files. If Autopsy does attach a number to the SAM, SYSTEM, or SOFTWARE hive name in the export folder, you will need to navigate to your case export folder and then right-click on each hive and select Rename. Rename each one to their exact name without the numbers.

Once you have the registry hives exported, open the Registry Explorer tool and click File►Load Offline Hive.
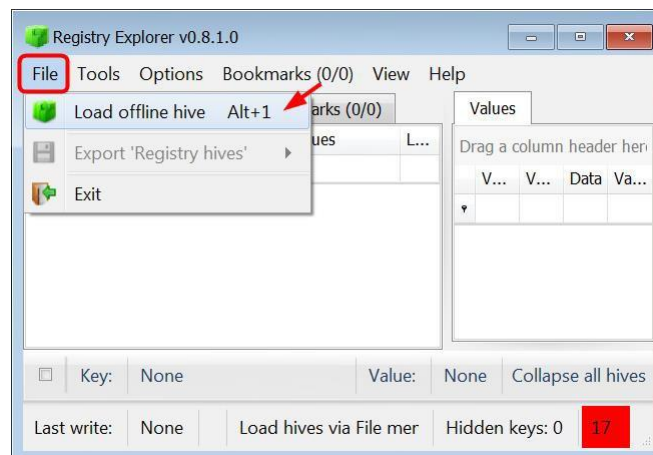
Figure 4-7 – Load Offline Hive in Registry Explorer

Navigate to where you exported the registry hives and select SOFTWARE hive to open. Once the tool opens the SOFTWARE hive, you need to go to the following subkey:

```
Microsoft\Windows NT\Current Version
```
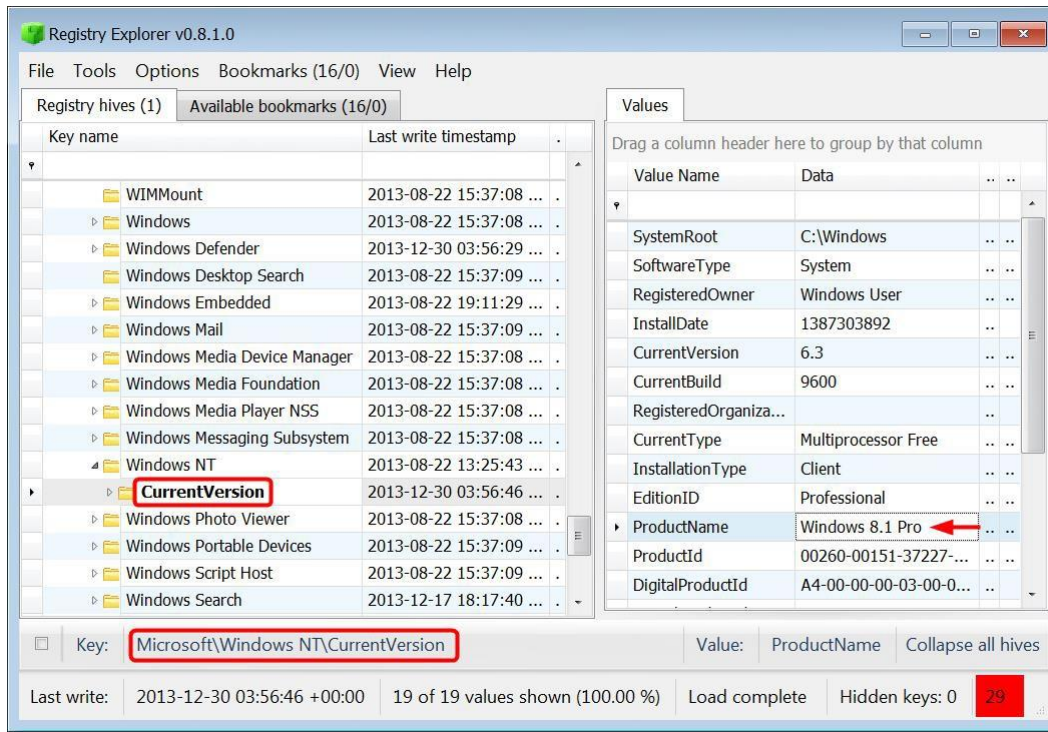

Figure 4-8 – Operating System in SOFTWARE

Time Zone

While Autopsy already pulled the operating system information with its module, there is some information in the registry that it does not pull. To find the time zone information in the registry, you will need to look at the SYSTEM hive. Open up the SYSTEM hive with Registry Explorer.
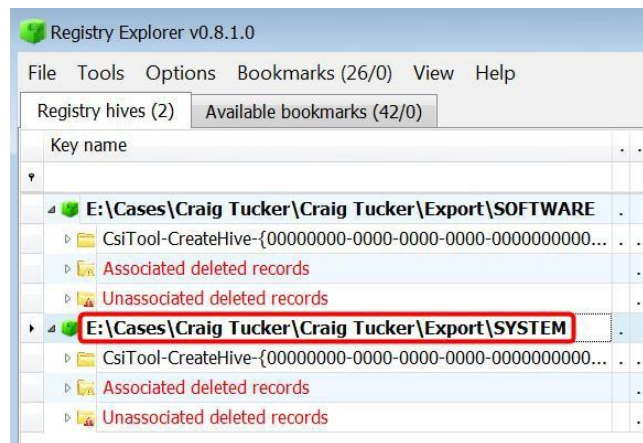
Figure 4-9 – Open SYSTEM Hive in Registry Explorer

Note: When navigating through Registry Explorer and the subkeys, always look under the top key "CsiTool-CreateHive". From there, navigate to the subkey path you are directed to.

Once you have the SYSTEM hive opened, navigate to the following subkey:

`[CurrentControlSet]\Control\TimeZoneInformation`

You will notice a subkey called ControlSet001. In other images, you may see two or more subkeys with the name ControlSet, such as ControlSet002 and ControlSet003.

If there are multiple control sets in SYSTEM, then you need to know which one is current. You can navigate to the Select subkey and it will show you a value for the current control set. In this case, it is showing 1 as the current control set.
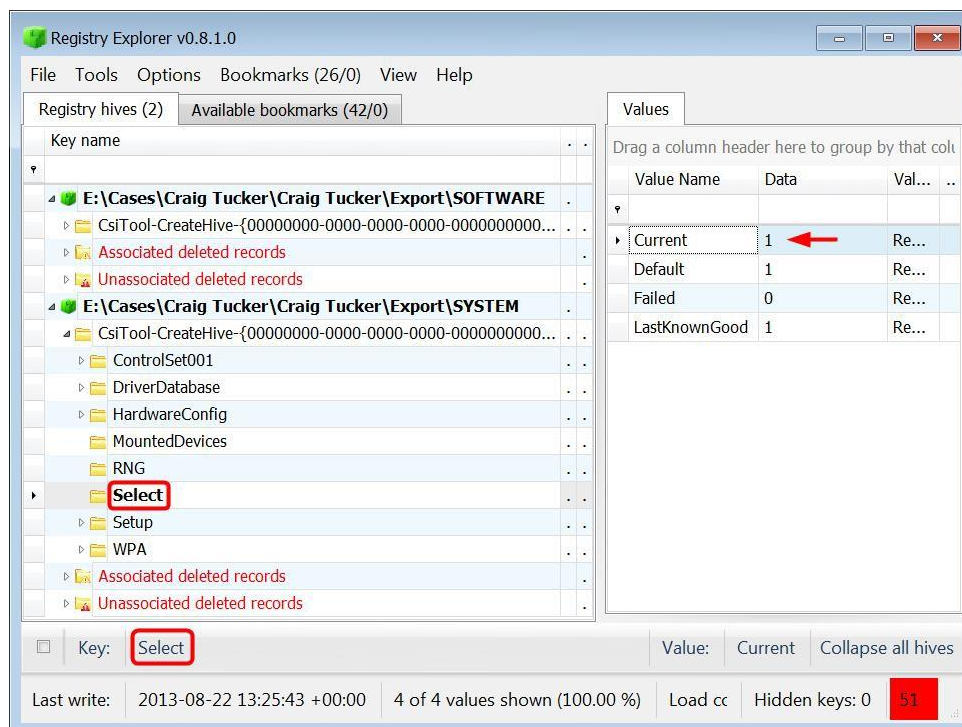
Figure 4-10 - Current Control Set in SYSTEM

Now that you know the current control set, navigate to:

`ControlSet001\Control\TimeZoneInformation`

Under TimeZoneInformation there are two important values to look at. The first value is the TimeZoneKeyName, and Registry Explorer decodes the value data to plain text. The other value is ActiveTimeBias, and it shows how many minutes the system is off from UTC. For this computer, it's 480 minutes off from UTC. If you divide that by 60, you get 8 hours, which is the Pacific Standard Time Zone (see Figure 4-11).
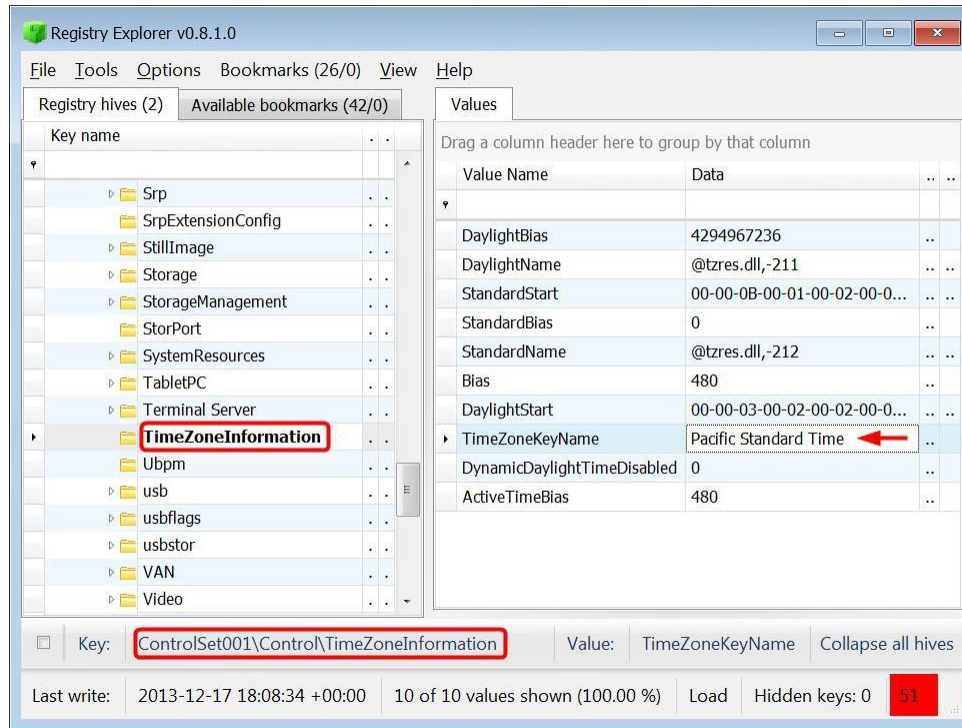
Figure 4-11 - TimeZoneInformation Subkey in SYSTEM

Identify Computer Users

The next section you will want to focus on when looking at registry data is identifying the computer users.

Understanding who was using the computer is a key part of your analysis. If your suspect was the only one that had access to the computer, then it makes it much easier to tie that person back to any activity on the computer. However, if other people were using it, you need to know who had access to what and which user account you need to focus on.

To view the user account information, select on Results►Extracted Content►Operating System User Account. There are several users listed, but if you remember from the User Profiles section, most of these are default accounts and default security identifiers (SIDs). In this case, there is only one user account, which is Craig. This user account has a SID of "S-1-5-21-1049150138-4017234595-3791460656-1001" and the RID is "1001" (see Figure 4-12).
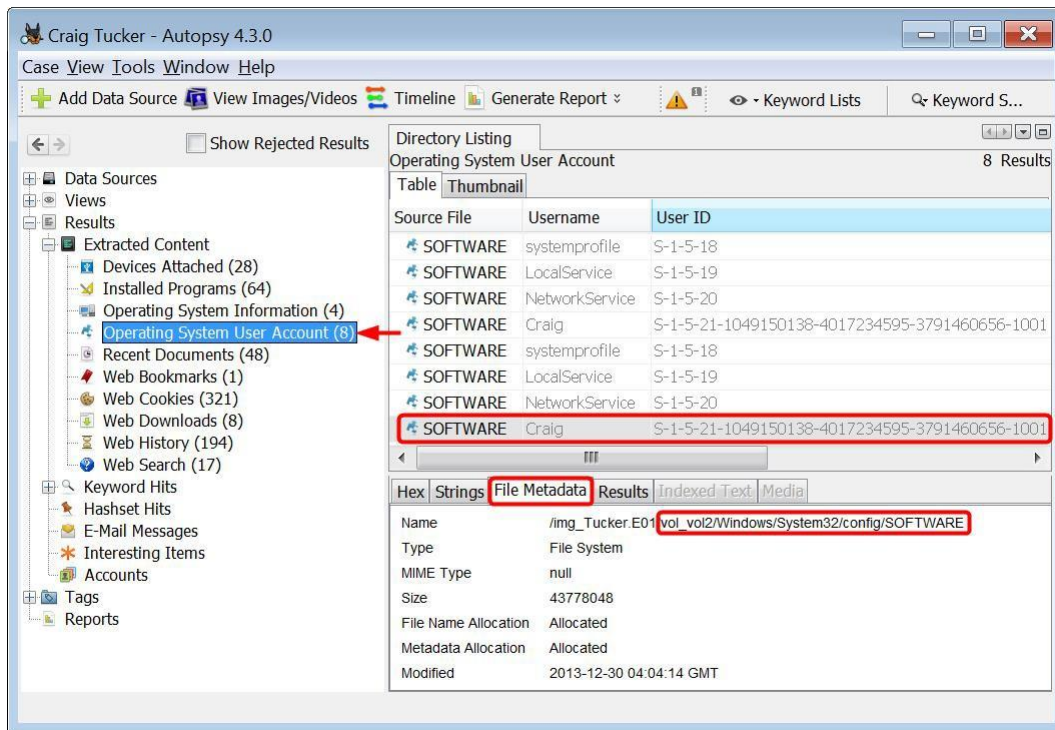
Figure 4-12 – User Account Information Extracted from SOFTWARE Hive

Note: There are duplicate entries for the user accounts because there are backups for each registry hive.

To find more information that Autopsy does not extract from the registry on users, look at the SOFTWARE hive in Registry Explorer. You need to navigate to the following subkey:

```
Microsoft\Windows NT\CurrentVersion\ProfileList
```

Under the ProfileList, there are four subkeys. The names of these four subkeys are the SIDs. The first three SIDs are defaults, and the last one is the user (see Figure 4-13).
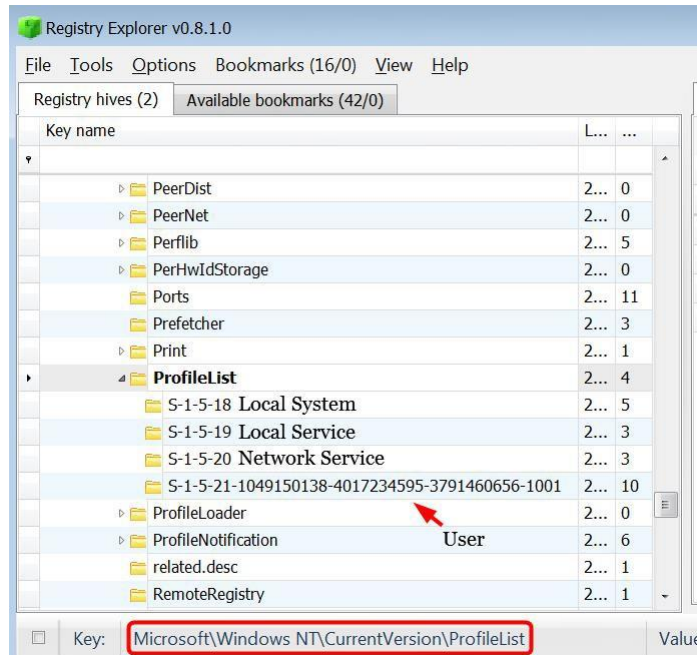
Figure 4-13 - User Profiles in SOFTWARE

In this case, there is only one user account with a SID of "S-1-5-21-1049150138-4017234595-3791460656-1001" and the RID is "1001". You can easily identify this profile to the user account called Craig by looking at the ProfileImagePath value.
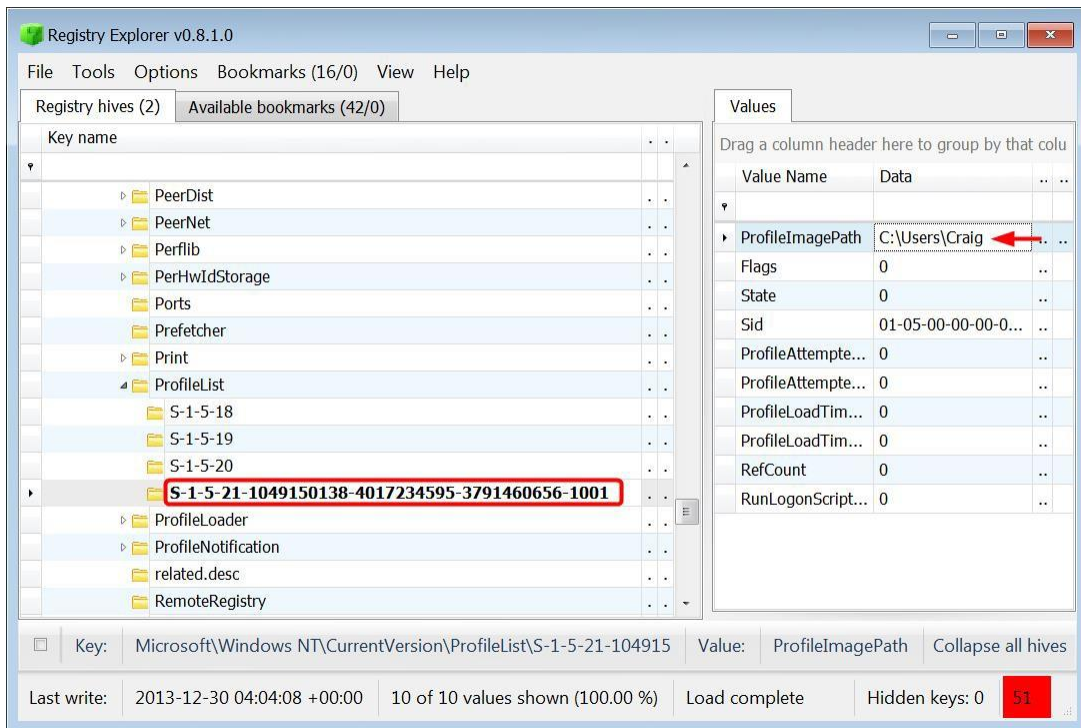
Figure 4-14 - User Craig's SID

The next place you can look at user accounts is the SAM hive. This hive is the Security Account Manager (SAM). You already exported this hive from Autopsy, so go ahead and open the hive in Registry Explorer. Go to the following subkey of the SAM hive:

```
SAM\Domains\Account\Users
```

Under the Users subkey, there are 3 subkeys listed. These subkeys are the hex values of the user's relative identifier (RID). If you were to convert these hex values to decimal, they would decode as the following:

000001F4 = 500

000001F5 = 501

000003E9 = 1001
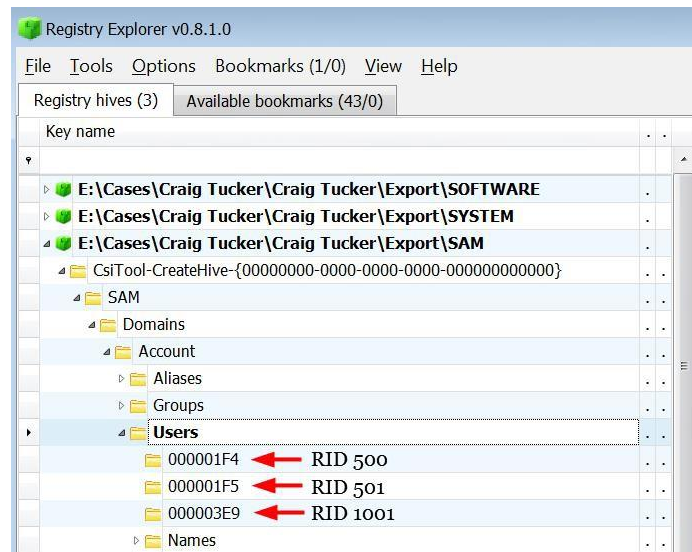
Figure 4-15 - User Profiles in SAM Hive

Since you already know that the actual user account, Craig, has a RID of 1001, select the 000003E9 subkey. This subkey stores a lot of information about the user account Craig. Information such as if the user account is disabled, how many times they logged in, and if the account has a password is mostly embedded within the values named F and V

Login Password

When a user sets a login password in Windows, the password is not stored in clear text. A hash value of the password is stored within the SAM hive in the V value.

From a security standpoint, Microsoft did not just store a hash value of the user's password. As an added security measure to secure the NTLM hashes, the hash values are protected with Syskey. Syskey is basically an encryption key that is scattered throughout the SYSTEM hive, which is unique to a given system AND user.
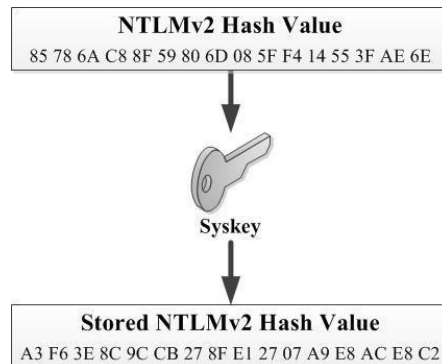
Figure 4-16 - Password Hash Value is Encrypted with Syskey

When a user types his password at the login prompt, the password is then hashed and compared against the stored hash in V. If the hash values match, then the user will successfully login to the operating system.

You can attempt to break the user's password by using a freeware tool called Ophcrack. This tool will also help determine which user accounts are password protected. The newest version of this tool (3.7) can be downloaded from:

```
http://ophcrack.sourceforge.net
```

To use Ophcrack and attempt to break the user's login password, you need to first export out the SAM and SYSTEM hives. Ophcrack uses the encrypted NTLMv2 hash value from the SAM hive and Syskey from the SYSTEM hive to reveal the actual NTLMv2 hash value. Once you have an actual hash value, Ophcrack will compare it to a rainbow table to find the password.

Note: A rainbow table is a pre-calculated dictionary full of hash values. Each hash value matches a password combination. Ophcrack uses the tables to compare the hash value stored in SAM, and tells you the password that matches the hash value.

You will also need to download the Vista free rainbow table from Ophcrack's website under the Tables tab (see Figure 4-17).
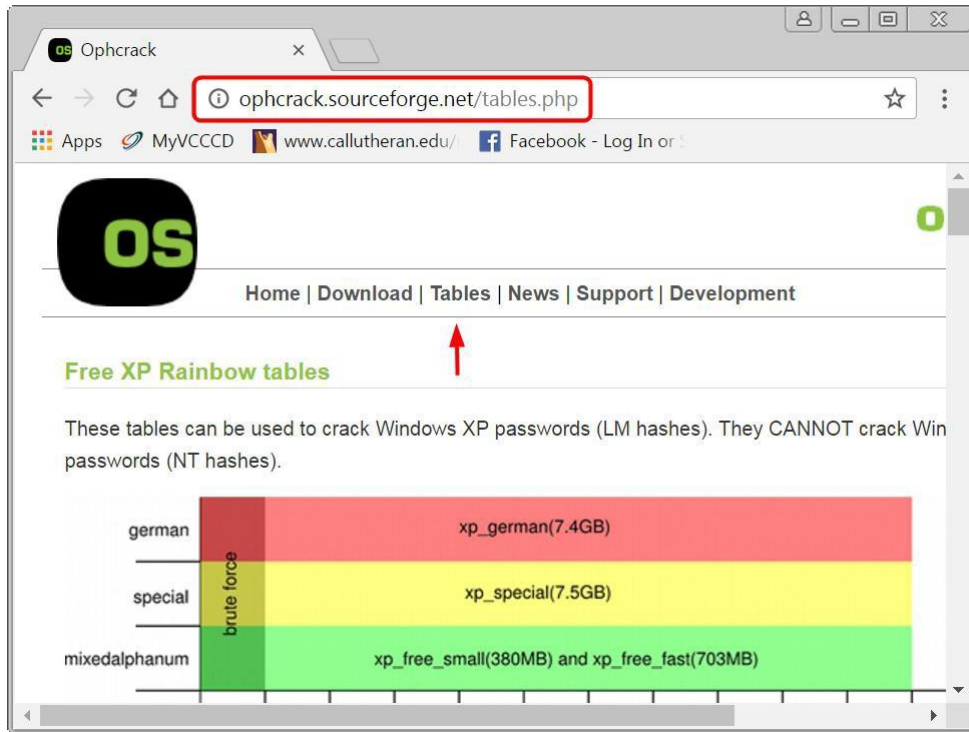
Figure 4-17 – Install Vista Free Table From Ophcrack's Website under Tables Tab

Open the Ophcrack tool and click Load►Encrypted SAM.
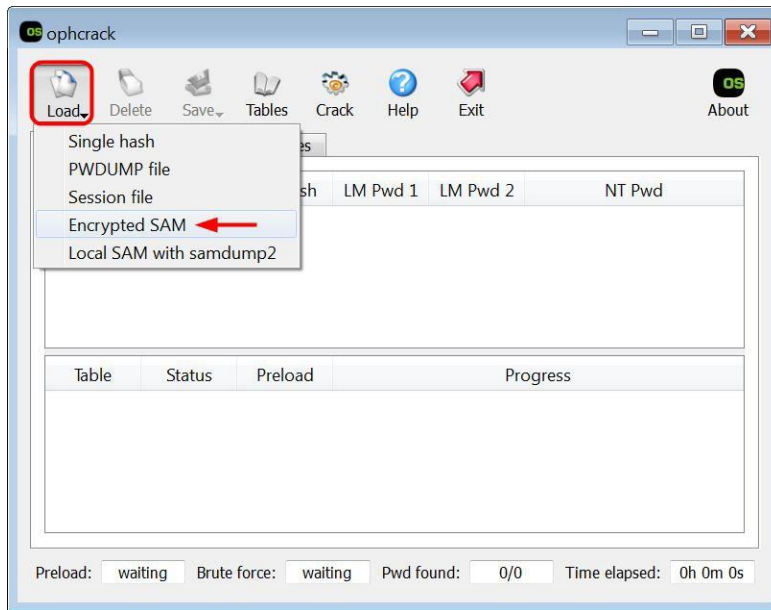
Figure 4-18 – Click Load Encrypted SAM in Ophcrack

Ophcrack will open a window for you to navigate to your case export folder. Highlight the Export folder and click Select Folder (see Figure 4-19).

Note: Make sure you took out the numbers in the SYSTEM and SAM hive and renamed them to just SYSTEM and SAM. Ophcrack will not recognize the files if they have numbers in the name.
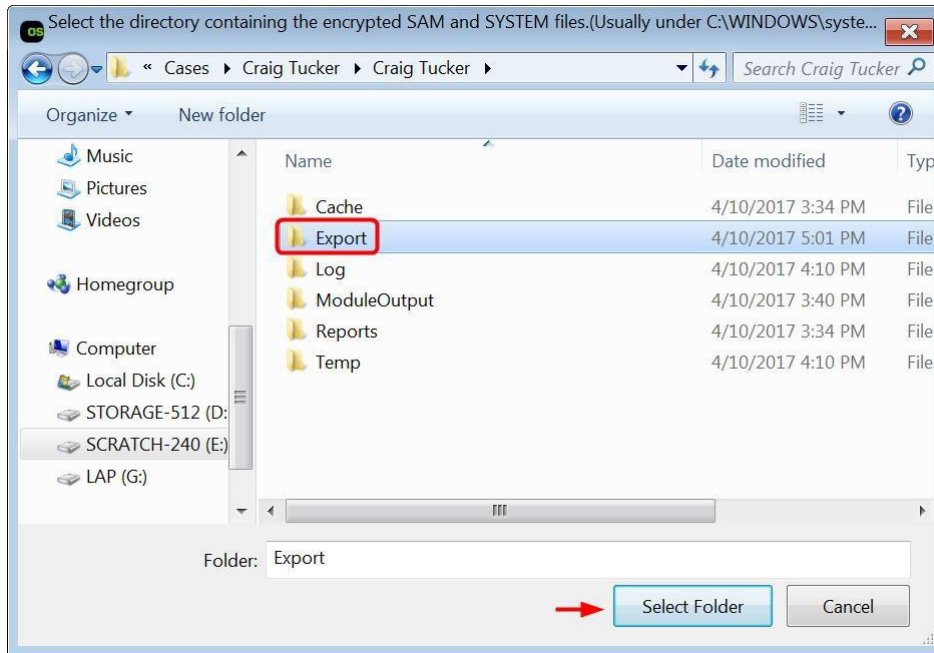
Figure 4-19 – Highlight Export Folder and Click Select Folder

After it loads, Ophcrack will show three users. The first two are the disabled Administrator and Guest user accounts. The third user account is Craig, and his decrypted hash value is shown as "85786ac88f59806d085ff414553fae6e." Before you crack Craig's login password, you need to install the Vista Free rainbow table. Click Tables in the top bar of Ophcrack. A Table Selection window will open and you need to highlight the Vista Free and then click Install.
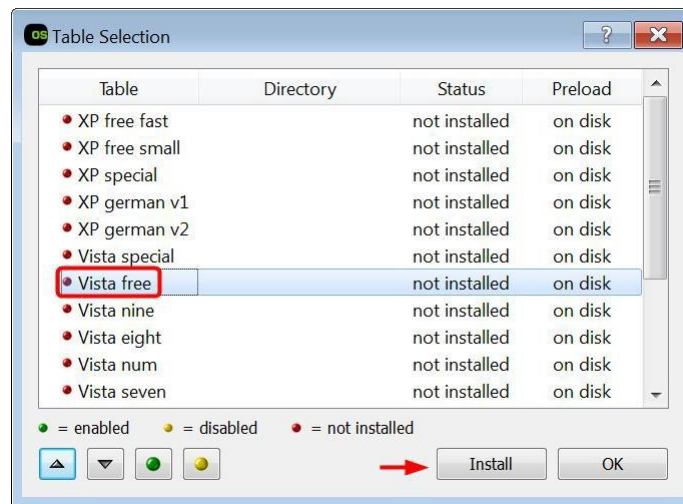
Figure 4-20 – Highlight Vista Free Table and Click Install

After clicking Install, navigate to where you downloaded the Vista free table from Ophcrack. You want to then click Select folder on the folder that you extracted from the downloaded zip from Ophcrack (see Figure 4-21).
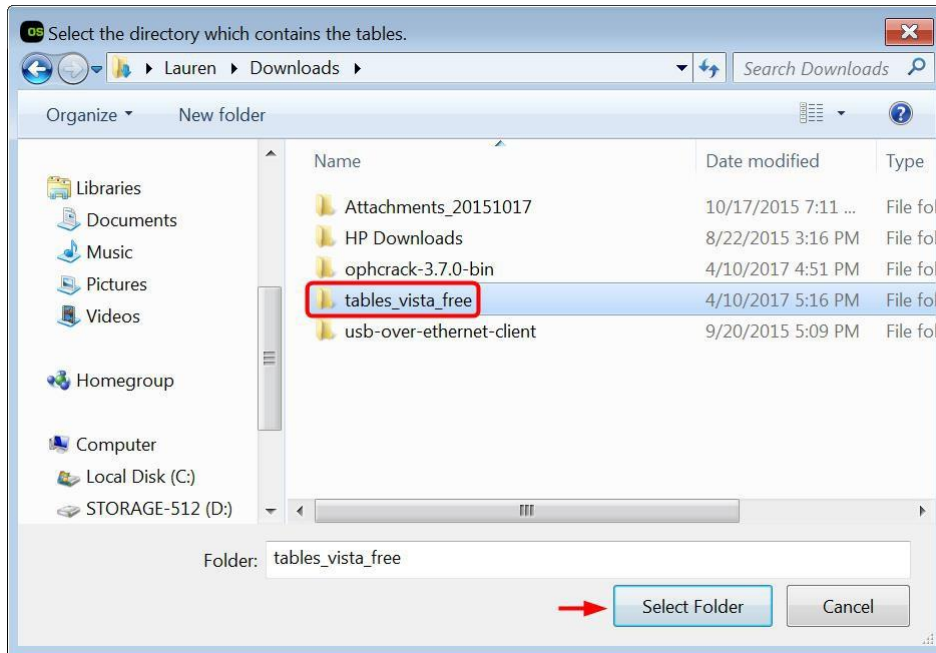
Figure 4-21 – Select Extracted Folder from Downloaded ZIP File and Click Select Folder

On the Table Selection window in Ophcrack, click OK. On the main Ophcrack window, you should see Vista free under Tables now. Click the Crack button in the top bar to crack Craig's login password.
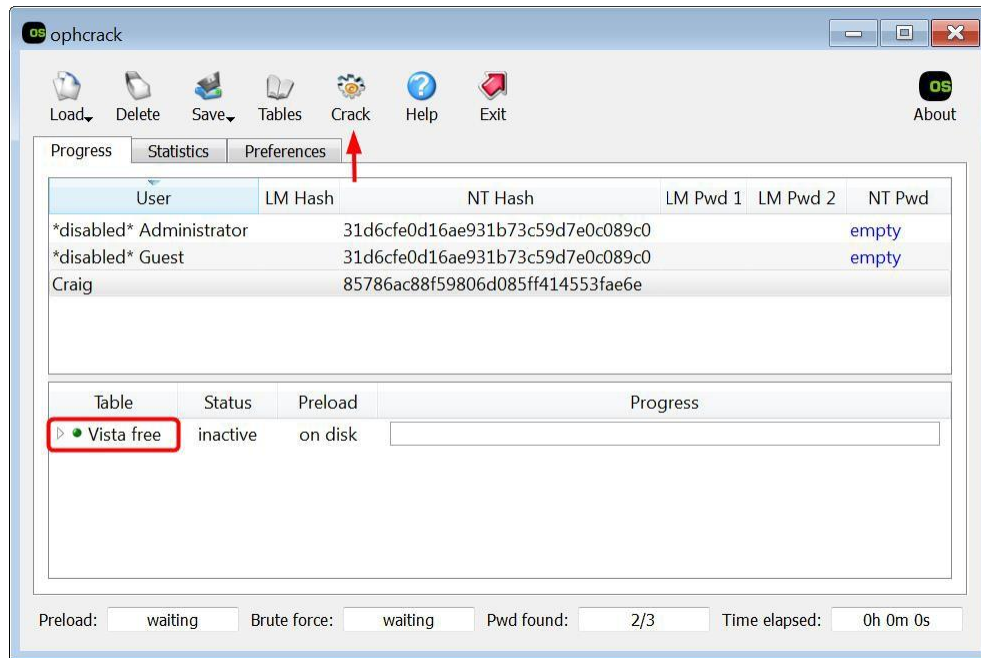
Figure 4-22 – Click Crack

If Ophcrack successfully finds a match, it will report back that hash value's matching password. In this case, Craig's password is hungry123. Knowing this password may help you break other password-protected files.
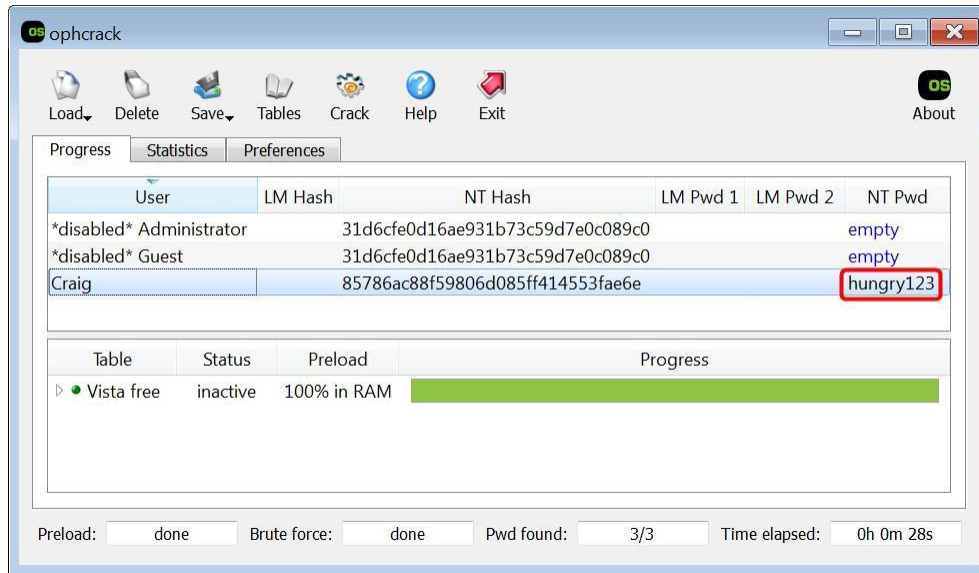
Figure 4-23 - Craig's Login Password Cracked

Note: Craig's login password "hungry123" is a very simple password and that is why you are able to break it with a smaller rainbow table. If the password had upper case letters, symbols, and was longer, you would need a much larger rainbow table to break the password, and it would take much more time to crack.

CAL POLY
California Cybersecurity Institute

Computer Forensics CCIC Training
Chapter 5: Starting Phase 2

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

5

Starting Phase 2

Introduction

During the Phase 2 Analysis, you will start to take a deeper dive into the forensic image to find specific evidence based on your case. The following steps are common areas of analysis done with Windows systems, but these steps may not be useful in every case. First, you will typically want to start by looking at where the user stored their personal data, what files they recently opened, and if there are any deleted files. You will also look to see if the user stored any personal data on external storage. After that, you will go through the suspect's email, Internet history, and chat logs. This phase will finish with a quick look for any evidence of data hiding and you will determine what programs the user installed. This more in depth phase will also cover how you can create a simple timeline and report your findings.

This chapter will focus on the first part, which is personal data. Users can save their pictures, documents, and videos in almost any location on the computer. However, you always want to first check the Windows default Desktop, Documents, Pictures, and Videos folder since a large majority of users store data in these folders. You also want to look at the Downloads folder and any cloud storage user folders. These folders will sometimes show what personal data the user downloaded or uploaded.

Personal Documents and Photos

Go to the Users folder. Under this folder there are five user folders. However, as you remember from the SAM and SYSTEM hives, there is only one true and active user profile, and that is Craig. The other folders are default account folders.

Under the Craig user profile folder, there is a file called NTUSER.DAT. If you remember from the registry section, the NTUSER.DAT file is the profile registry hive. Every user account has one, and it contains information specific to that user, such as their start page in Internet Explorer, desktop wallpaper, and information about programs they installed. You will go through Craig's NTUSER.DAT file later.

Since Craig is the only active user account for this computer, you can focus your attention on that user account. Navigate to Craig's Documents folder, which is located in:

```
C:\Users\Craig\Documents
```

This is a default location where many users store their documents. This does not mean that every user will put their documents there, but it is a good place to look.
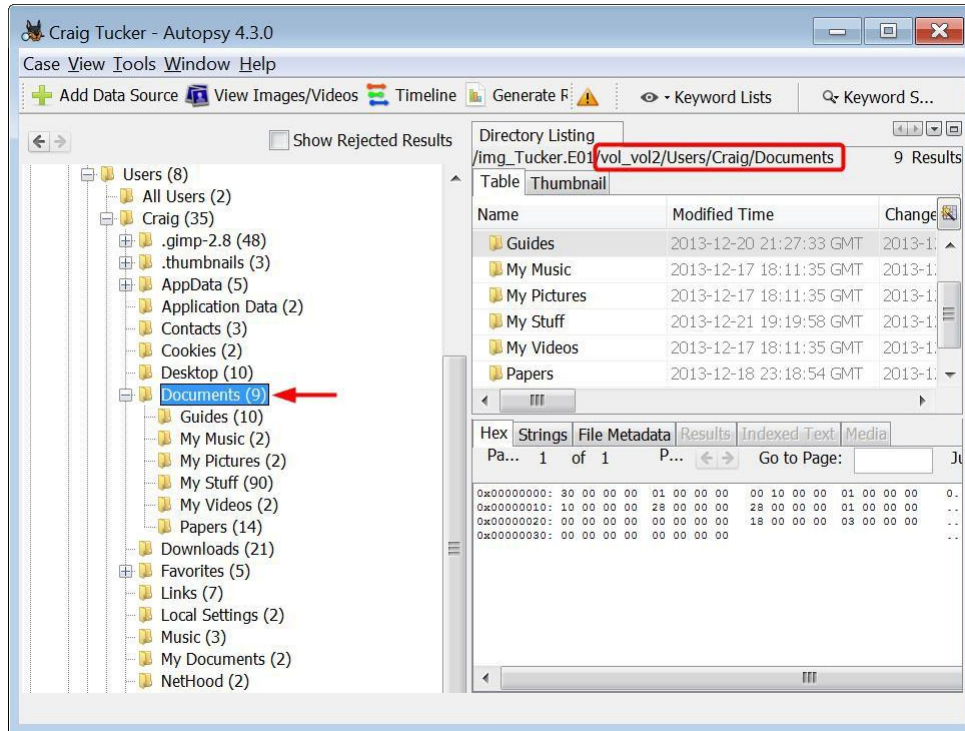
Figure 5-1 – Craig's Documents Folder

As you can see, Craig has several subfolders under his Documents folder. In the Guides subfolder, he has documents describing how to make and use coupons.

Tag

When you have files of interest in your case, you may want to tag them so you can easily find and review them later. You can tag these files by clicking a file at the top of the list in the table pane and then press the Shift key while left clicking the last file in the table pane. This will highlight all the files in between the two you clicked. Once you have all four files of interest highlighted in the Guide subfolder, right-click one and select Tag Files►Tag and Comment.
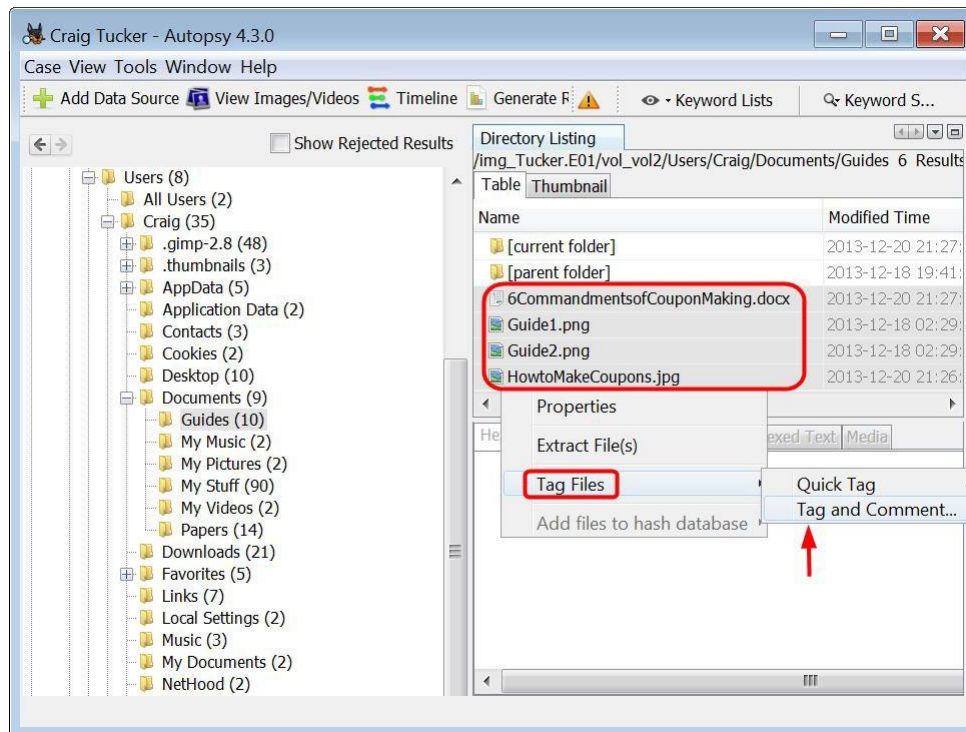
Figure 5-2 – Highlight Files in Guide Subfolder, Right-Click and Select Tag and Comment

A Create Tag window will open and you can use Autopsy's default Tag, which is Bookmark. You can also create your own preferred tag name by clicking the New Tag Name button. You can also type a quick comment if you'd like to help you remember later why you tagged a file. Click OK.
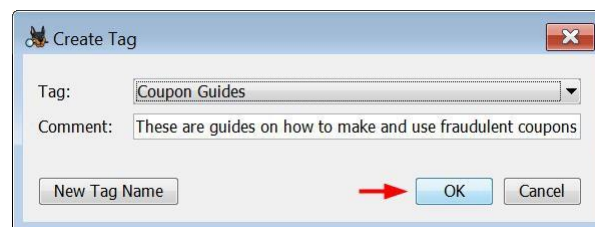
Figure 5-3 – Set Tag Name and Comment and Click OK

When you want to view your tagged files later, simply scroll down to Tags in the left pane. This is a quick and easy way to mark files that relate to your investigation, and it helps you remember and report all of your findings at the end of your investigation (see Figure 5-4).
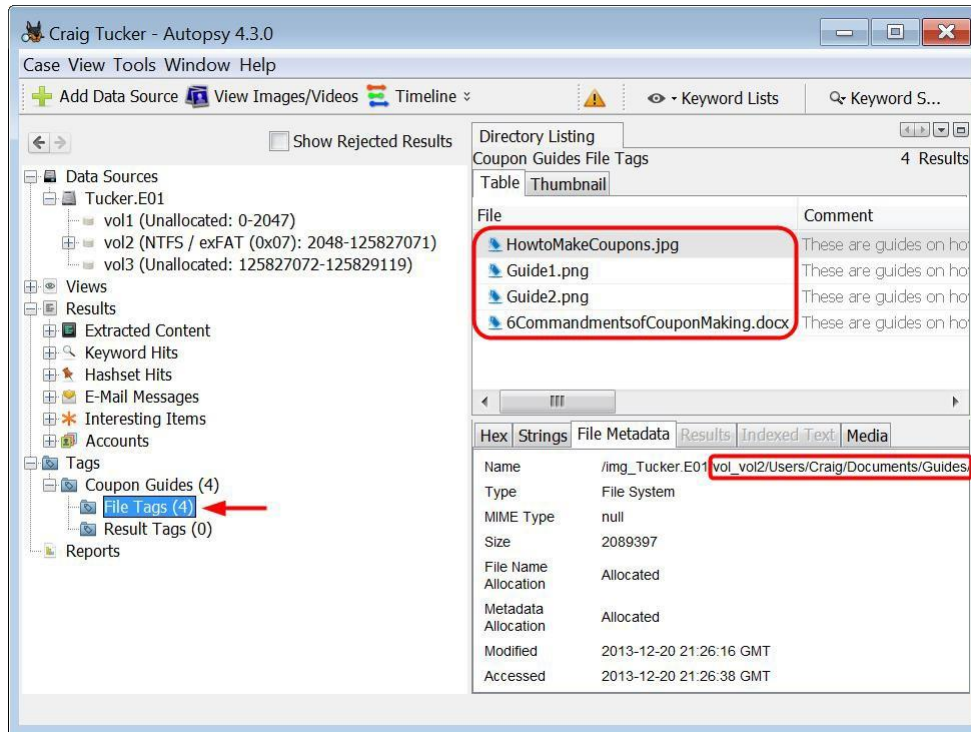
Figure 5-4 – View Tagged Files in Tags

Take a look at Craig's other subfolder under Documents called My Stuff. There are several pictures of coupons in this folder. Go ahead and add these files to your same Tag or a new one.
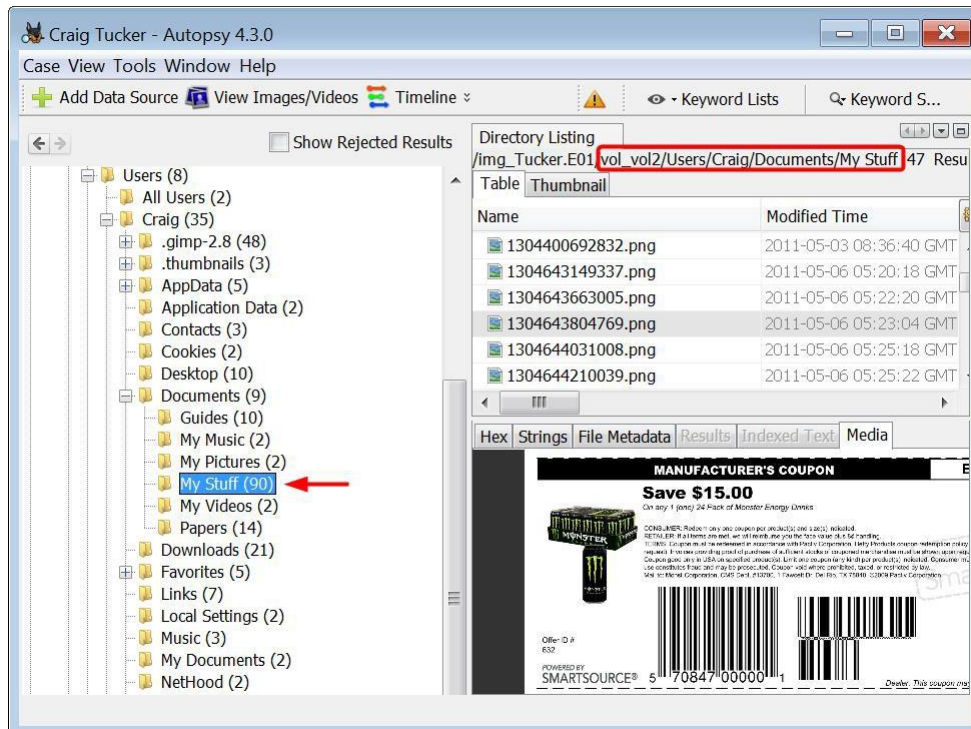
Figure 5-5 – Tag Coupon Files in Craig's My Stuff Folder

Zone ID

In the My Stuff folder, you will notice that one graphic file, Whopper.jpg, is different than the other files. Autopsy shows in the table pane that this file also has another entry called Whopper.jpg:Zone.Identifier. Highlight this file and you will see in the Hex view pane or the Strings view pane that it contains the text "[ZoneTransfer] ZoneId=3".
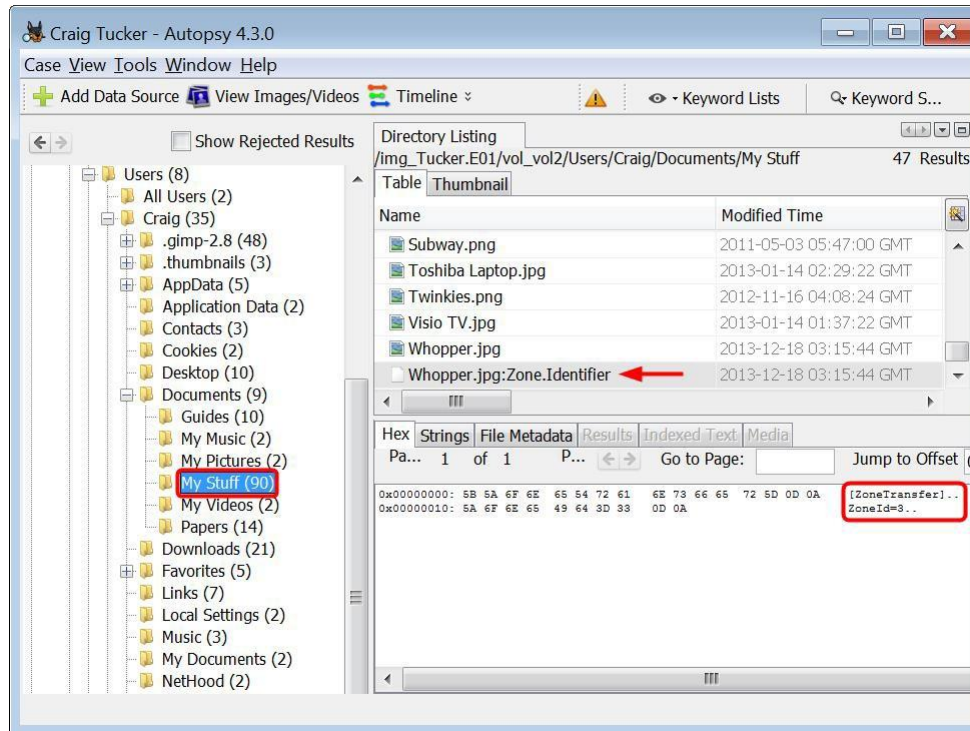
Figure 5-6 - Zone ID=3 in Whopper.jpg:Zone Identifier

Starting with Windows XP SP2, Microsoft added an Alternate Data Stream (ADS) to a file that was downloaded from the Internet to a NTFS volume. Think of this as a security flag used to determine the source of a file. The ZoneId value of 3 means that the file was downloaded from the Internet and it is potentially unsafe. The values could be from other zones, such as the following:

MyComputer	0
Intranet	I
Trusted	2
Internet	3
Untrusted	4

From an analysis perspective, a file that has an ADS called Zone.Identifier with ZoneID=3, you know that the file originated from the Internet and is direct evidence of downloading a file.

Note: Any files that are extracted from a downloaded ZIP will have an ADS added to the file with a Zone ID of 3.

Personal Documents and Photos (Continued)

The next place to look for personal data is the Pictures folder. Navigate to:

```
C:\Users\Craig\Pictures
```
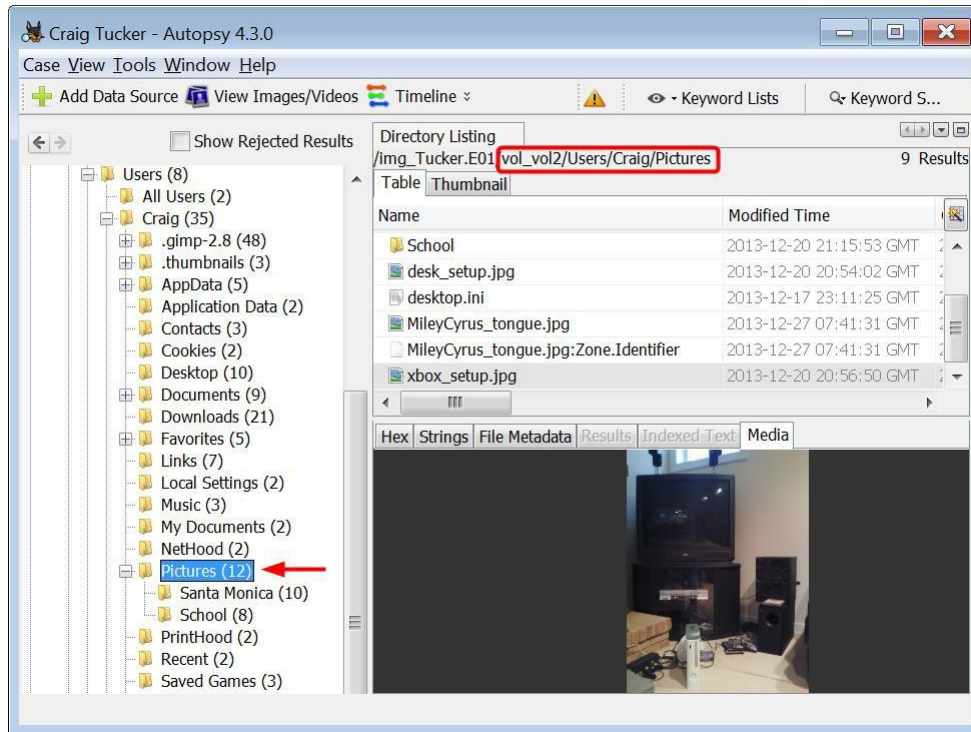

Figure 5-7 – Craig's Pictures Folder

As you can see, the only data in the folder is personal pictures, and they are unrelated to your case.

Next, navigate to Craig's desktop (see Figure 5-8). This is under:

```
C:\Users\Craig\Desktop
```
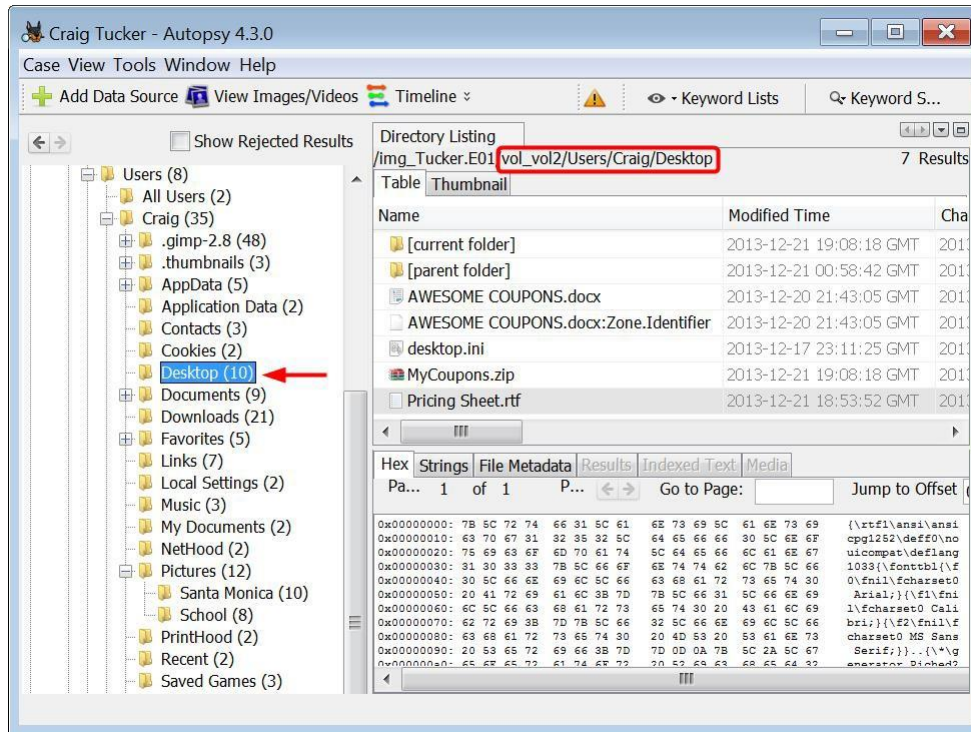
Figure 5-8 – Craig's Desktop

Craig only has a few documents on his desktop. If you want to view document or some email type files within Autopsy, you will need to download the Multi Content Viewer 3rd party module. This can be downloaded from:

```
https://github.com/lfcnassif/MultiContentViewer/releases/tag/v1.0-beta
```

After you download the .nbm file for the Multi Content Viewer module, you need to install it. To install a 3rd party module, you need to click Tools►Plugins.
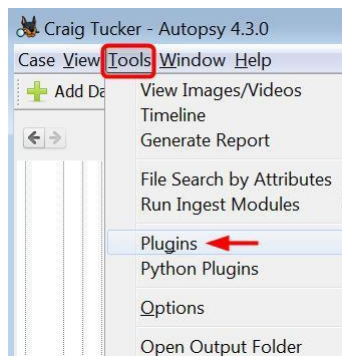
Figure 5-9 – Click Plugins under Tools

When the Plugins window opens, click the Downloaded tab at the top of the window. Click the Add Plugins button (see Figure 5-10).
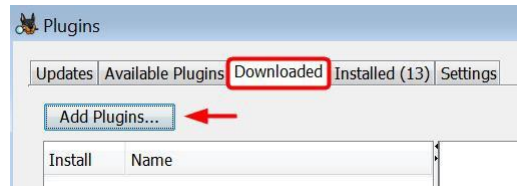
Figure 5-10 – Click Add Plugins under Downloaded Tab

An Add Plugins window will open, and you need to navigate to where you downloaded the .nbm file. Select the .nbm file and click Open.
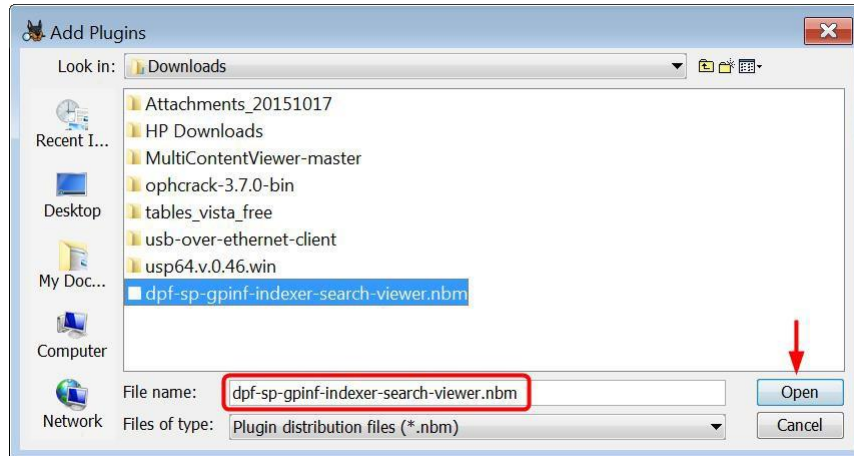
Figure 5-11 – Select nbm File and Click Open

The Multi Content Viewer plugin will now show up in the list. Click the Install button in the bottom left corner.
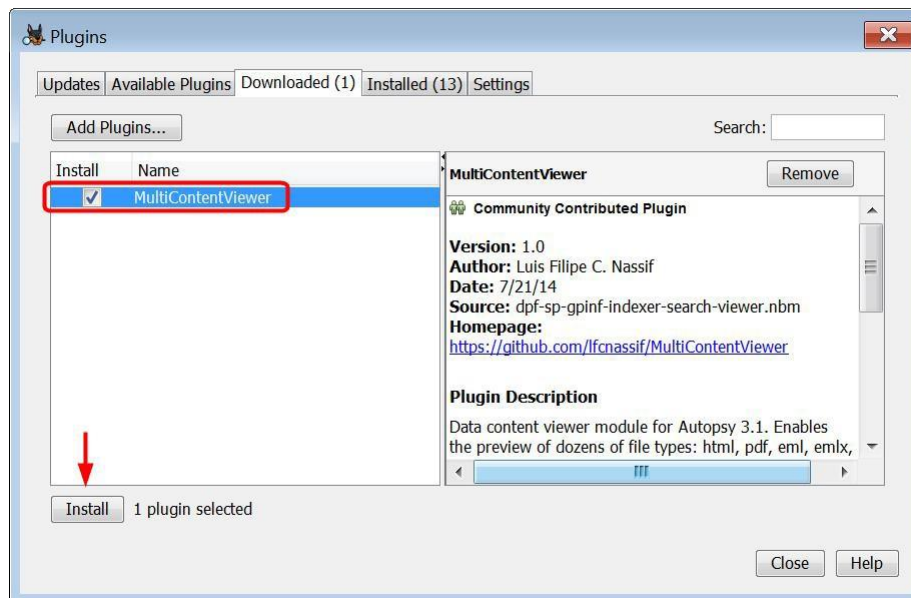
Figure 5-12 – Click Install on MultiContentViewer Plugin

Go through the steps to install the plugin. The last Plugin Installer window will prompt you to restart Autopsy. Select Restart Now and then click Finish (see Figure 5-13).
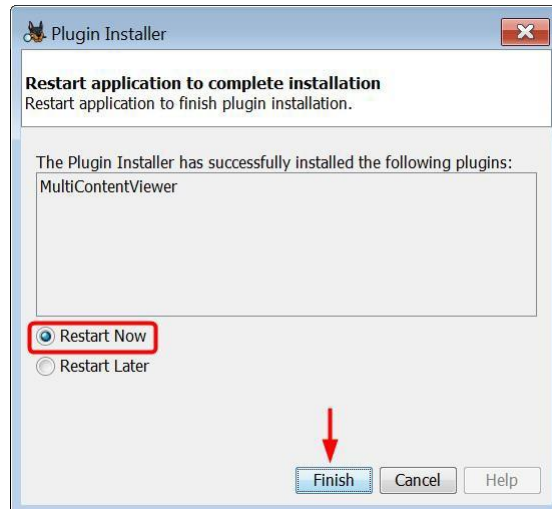
Figure 5-13 – Select Restart Now After Installing Plugin and Click Finish

Open up Autopsy again and navigate to Craig's Desktop folder. You can now view certain file types within Autopsy, such as the .rtf file on Craig's Desktop.

There are still some other files on Craig's Desktop of interest, such as the AWESOME COUPONS.docx and MyCoupons.zip files. First, let's try to open the AWESOME COUPONS.docx file. You are unable to view this file within Autopsy perhaps because it is password protected. To view this file, you need external software that can open and view docx files, such as Microsoft Word or Open Office. Right-click the AWESOME COUPONS.docx file and click Open in External Viewer.
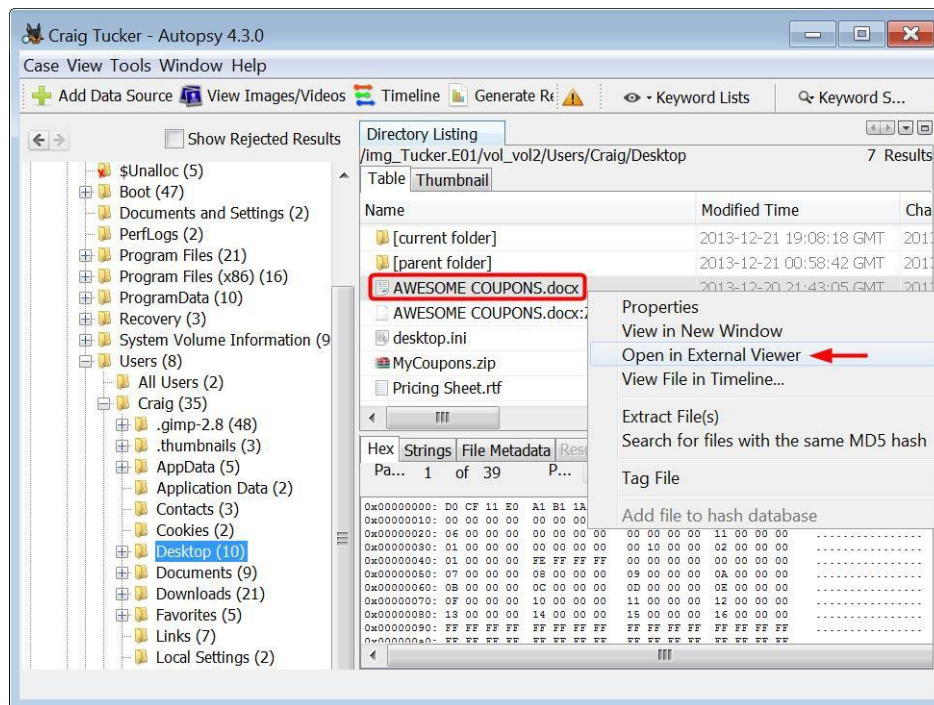
Figure 5-14 – Right-Click AWESOME COUPONS.docx and Select Open in External Viewer

Your default document viewer should attempt to open the file and you will be prompted with a Password window. We will come back to this password protected document later.
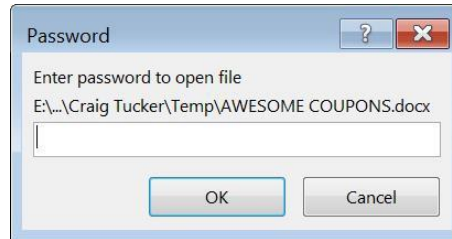
Figure 5-15 – Password Needed for AWESOME COUPONS.docx

Let's next try to open the MyCoupons.zip file. To open and view the contents of container files, such as zip and rar files, you need to run the Embedded File Extractor module. Click on Tools►Run Ingest Modules►Tucker.E01. When the Run Ingest Modules window opens, check Embedded File Extractor and then click Start.
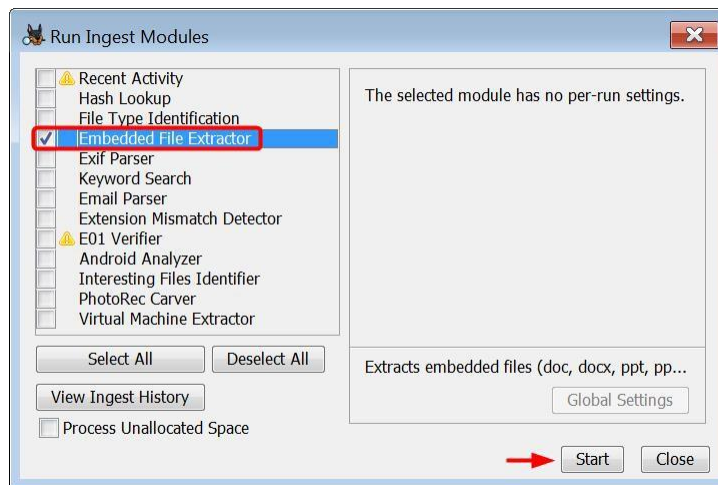
Figure 5-16 – Check Embedded File Extractor and Click Start

If you click on the Ingest Messages button in the top bar of Autopsy, you will see that the Embedded File Extractor module has detected an encrypted file (see Figure 5-17).
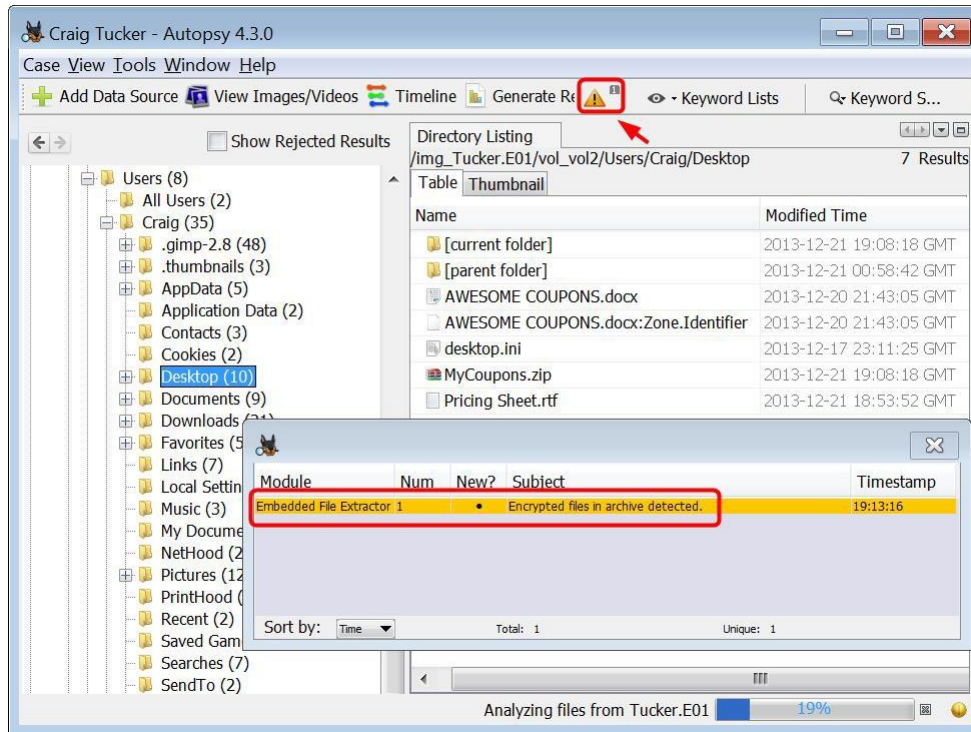
Figure 5-17 – Click Ingest Messages Button to View Encrypted Files Detected

If you click on this message in the module list, it will show that the MyCoupons.zip has encrypted files. We will come back to this file and the other encrypted docx file later.

Next, take a look at Craig's SkyDrive, now known as Microsoft OneDrive, (see Figure 5-18). This is located at:

```
C:\Users\Craig\SkyDrive
```
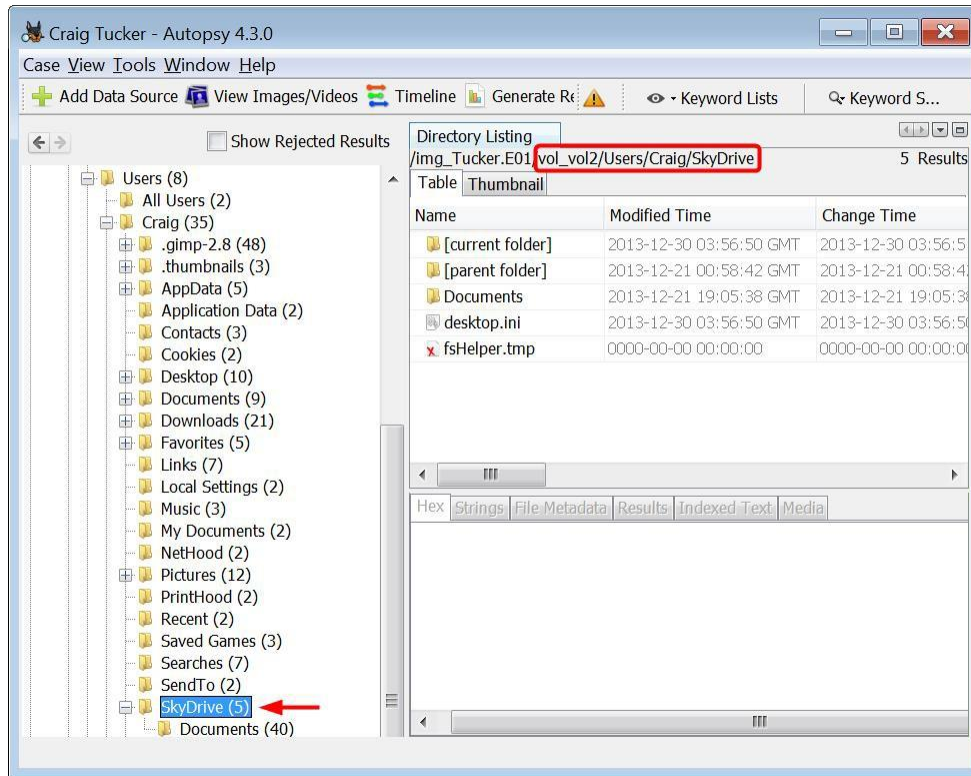
Figure 5-18 – Craig's Skydrive

When this drive was imaged, Microsoft still had Skydrive incorporated into the user's environment. Skydrive is now known as Onedrive, but its basic function is the same. When something is saved to Skydrive (Onedrive), it syncs to the Cloud and users can then access these files from other computers, tablets, or their phone. Users might not always save data to this location, but it's a good place to check.

Craig's Skydrive contains several coupons. Each coupon also has a Zone ID of 3, which means they have been downloaded from the Internet. You can tag these files for now to easily come back and review them later.

Now, navigate to Craig's Download folder (see Figure 5-19), which is located at:

```
C:\Users\Craig\Downloads
```

Users can change where they want their default download folder, so there might not always be data here. However, it is still a good place to check.
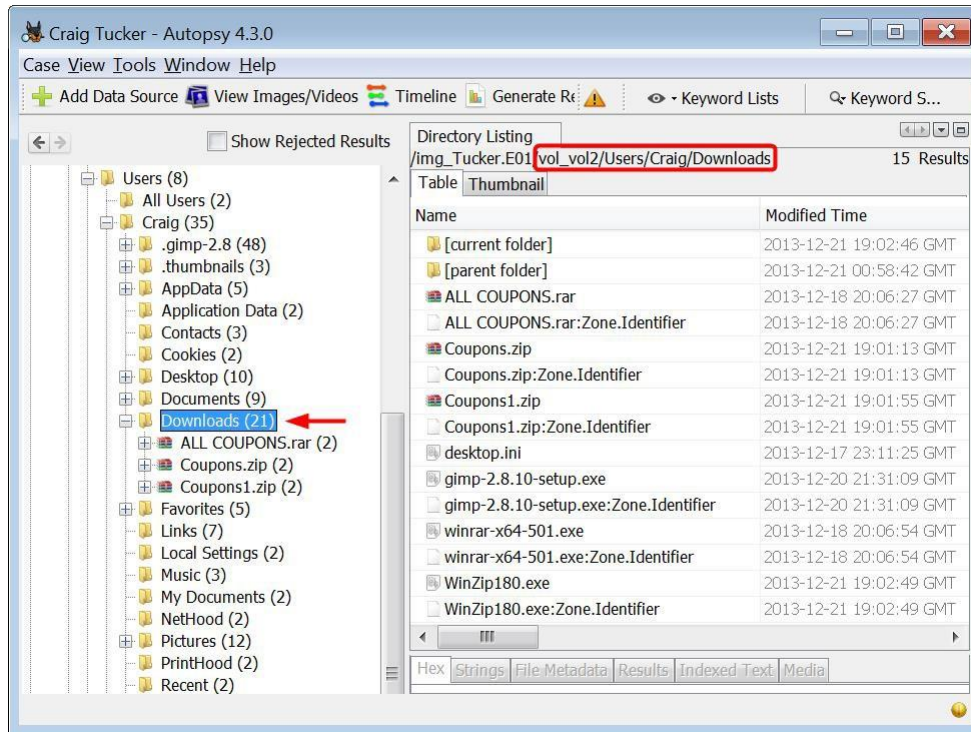
Figure 5-19 – Craig's Downloads Folder

You will notice that all six of the actual files listed in the Downloads folder have an ADS with Zone ID=3, which means they were also downloaded from the Internet.

In Craig's Downloads folder, he has a RAR file, two ZIP files, and three programs. You already ran the Embedded File Extractor module for the other zip file on his desktop, so you can now open and view the data in these compressed files. As you can see, these ZIP and RAR files contain several coupons. You can tag these files for now since we will come back to them later to determine where Craig downloaded them from.

Computer Forensics CCIC Training

Chapter 6: Recent Files

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

6

Recent Files

Introduction

From an investigative standpoint, you usually want to determine what files a user recently accessed. It gives you a perspective on how the user used the computer, and it also associates file activity back to the suspect. This will help demonstrate their knowledge about the existence of the files and show that they opened and viewed it. In this chapter, we will focus on link files and jump lists. Both of these artifacts will show you what files the user opened.

Link Files

You are going to first look in Craig's Recent folder. This is located in the following path for versions 7-10 of Windows:

`C:\Users\Craig\AppData\Roaming\Microsoft\Windows\Recent`
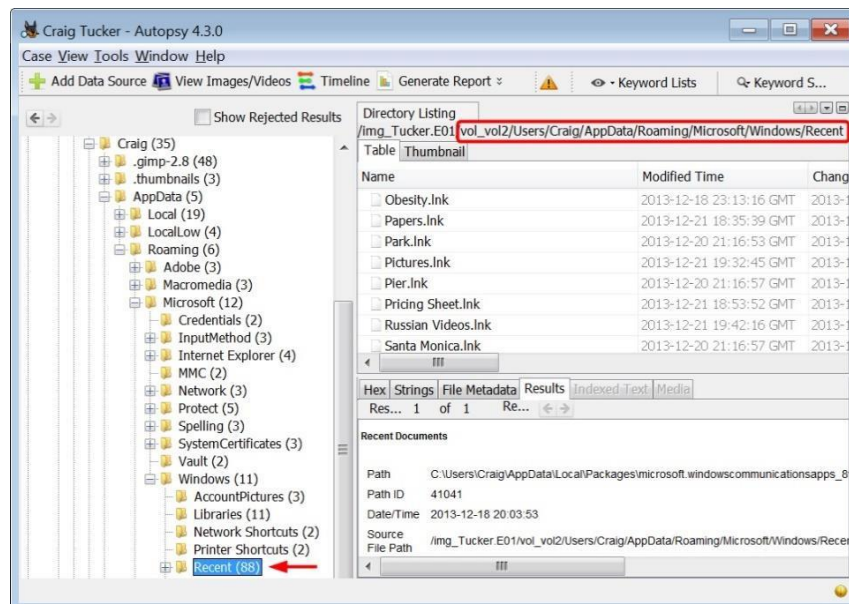
Figure 6-1 – Craig's Link Files in Recent Folder

This folder contains the user's link files. A link file, or LNK, is a Windows shortcut that points back to an original file. A link file is generally created when a file is first opened. Link files are important during analysis, because they show where files were located, when they were opened, and they contain date and time stamps associated with the file. If you look at Windows Explorer and go to the Recent folder, you can see your own link files.
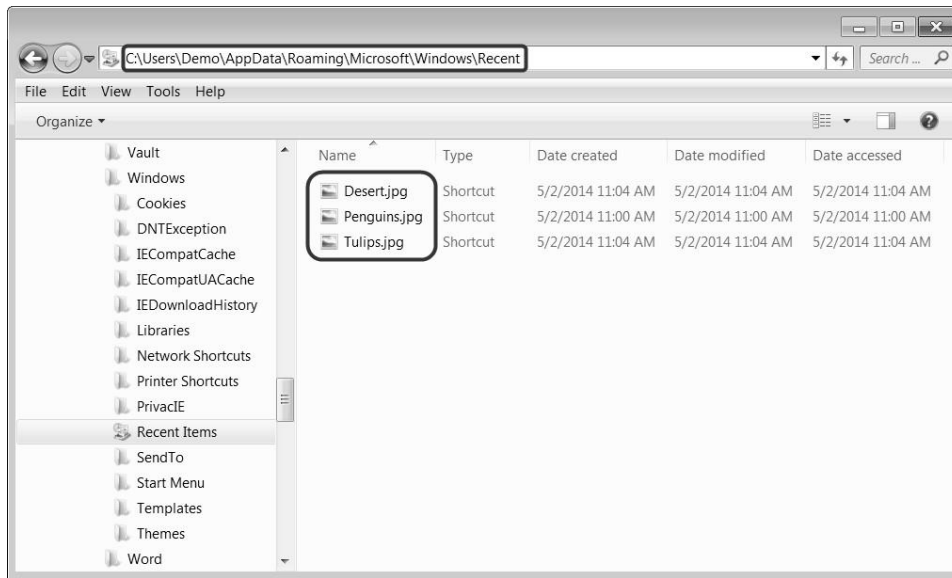
Figure 6-2 – Link Files in Windows Explorer

Note: To view the AppData folder since it is hidden, open Windows Explorer and click Organize►Folder and Search Options. Check Show Hidden Files, Folders, and Drives under the View tab. If you are on a Windows 8 or 10 machine, click the View tab on Windows Explorer and check Hidden Items.

If you right-click one of the link files and select properties, you can see the information about the link file (see Figure 6-3).
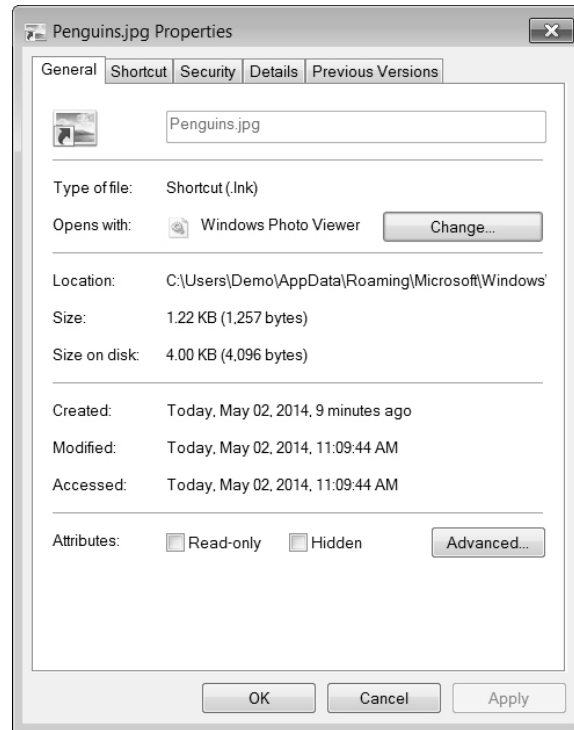
Figure 6-3 – Link File Properties

This link file is merely a pointer back to the actual file. It contains date and time stamps, the size of the file, and if you look at the Shortcut tab, you can even see where the file was located when it was opened.
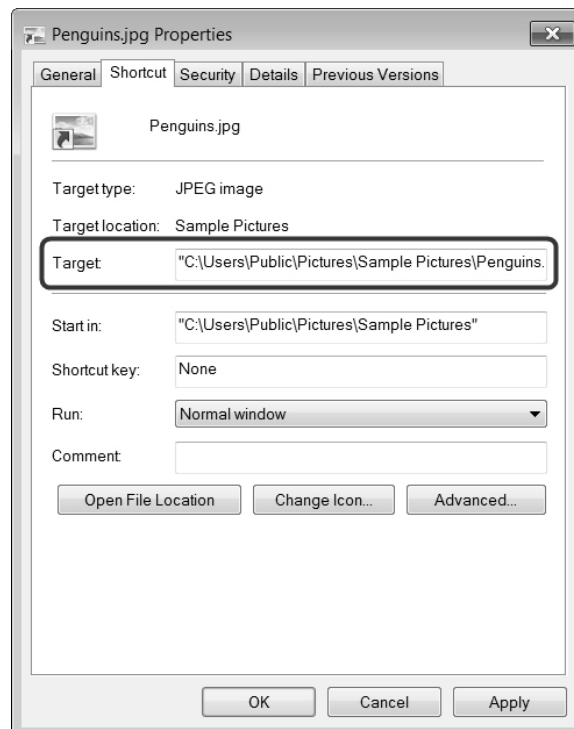
Figure 6-4 - Link File Pointing to Actual File's Location

Example 1 (File Opened Once)

Back in Autopsy, look at the link file called Pier.lnk and click on the Results view. Autopsy will show you the path of where Pier.jpg was stored when it was opened.

Figure 6-5 – Link File Shows Path of Pier.jpg

If you view Pier.lnk in Hex view, you can see that inside this link there is embedded data that points back to the original file that was opened.
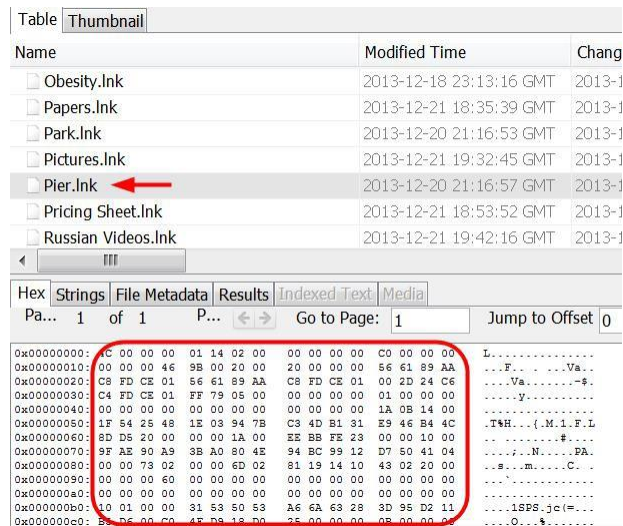
Figure 6-6 – Embedded Data in Pier.lnk

There are three date and time stamps EMBEDDED within the link file. The time stamps you see in the Hex view refer back to the file "Pier.jpg".

Embedded Time Stamps	Description
Creation Time (Yellow)	This is the time that the file (Pier.jpg) was created in that local path. If the file had been copied to that location, then the Creation date/time is when it was copied.
Last Access Time (Green)	Last access times have been disabled since Windows Vista. It keeps the same date as the Creation time (UTC), but there are some variables that can change or update it.
Last Write Time (Blue)	This is the time that the file (Pier.jpg) was last modified. This is not necessarily the last time it was opened.

Figure 6-7 – Embedded Creation, Last Access, and Last Write Times of Pier.jpg

To decode these time stamps, you are going to use the tool called DCode (Version 4.02a). You can download this tool at:

```
http://www.digital-detective.net/digital-forensic-software/free-tools/
```

Once you have DCode up and running, you need to copy the time stamps out Pier.lnk in hex view and paste them into Notepad.
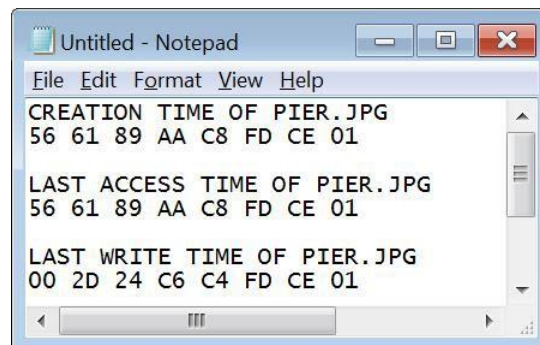
Figure 6-8 – Copy and Paste Embedded Time Stamps of Pier.lnk

In DCode, set the Decode Format to Windows: 64 bit Hex Value – Little Endian. Next, past the first time stamp (creation time of pier.jpg) into the Value to Decode. Hit the Decode button in the bottom right corner and you should see the decoded embedded creation time stamp (see Figure 6-9).
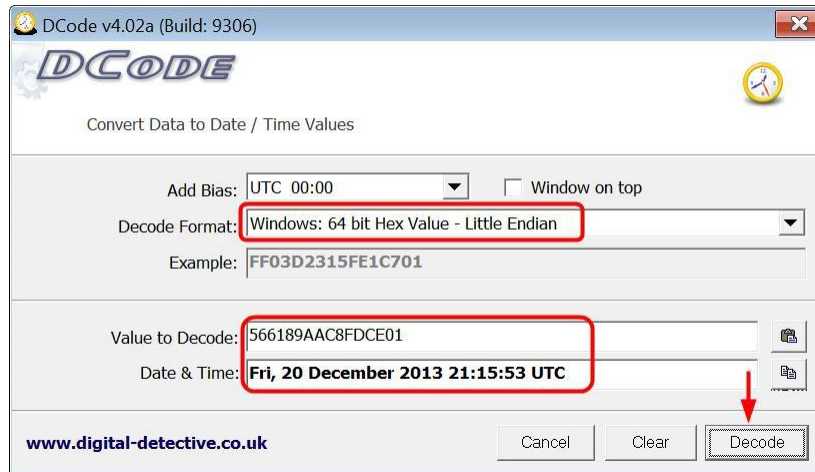
Figure 6-9 – Embedded Creation Time Stamp Decoded

Repeat this for the other two time stamps, and you should have the following date and time stamps:

Embedded Creation Time (UTC): Fri, 20 December 2013 21:15:53 UTC

Embedded Access Time (UTC): Fri, 20 December 2013 21:15:53 UTC

Embedded Last Write Time (UTC): Fri, 20 December 2013 20:48:02 UTC

Next, you need to look at the date and time stamps of the link file itself.

Figure 6-10 - Date and Time Stamps of the Link File

The time stamps in the table pane are about the link file itself and are separate from the time stamps embedded within the link file.

Link File Time Stamps	Description
Created Time	When a file is first opened, it creates a link file. The link file's Created time stamp is when the file (Pier.jpg) was FIRST opened.
Modified Time	This is the time when the file (Pier.jpg) was LAST opened. If this is the same as the Created time stamp, then you know that the file was only opened once.
Access Time	Once again, the accessed time is disabled in Windows Vista, 7, and 8. Accessed will be the same date and time as Modified.

As you can see in Figure 6-10, the Created and Modified time of the link file are the same. This means that the file (Pier.jpg) was only opened once.

Here is a timeline of the file Pier.jpg (All UTC):

12/20/13 at 20:48:02
File is Last Modified
(Embedded Last Write Time)

12/20/13 at 21:15:53
File Lands in Pictures Folder
(Embedded Creation Time)

12/20/13 at 21:16:57
File Lands in Pictures Folder
(Link Created and Modified)
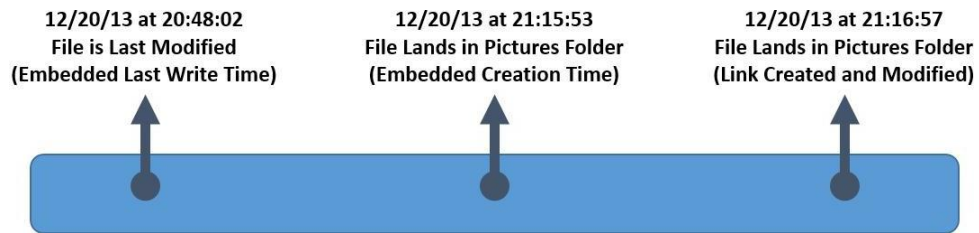
Figure 6-11 - Timeline of Pier.jpg Based on Link File

Since the last time this picture was modified is BEFORE the time it was created in that folder, it is likely that this file was copied to the Pictures folder.

Example 2 (Files Opened More than Once)

Take a look at the file called Cheetos.lnk and click on the Results view. Autopsy will show that this link file is pointing to a "Cheetos.jpg" in E:\Coupons. This is important to note, because this could mean that Craig had plugged in and used an external drive since it is found on something other than the C: drive.

Figure 6-12 - Link File Shows Path of Cheetos.jpg

Next, take a look at the embedded date and time stamps in the Cheetos.lnk file.
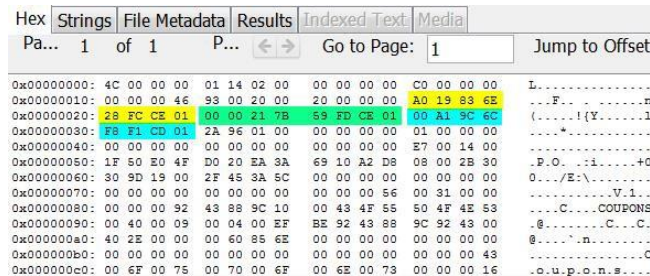
Figure 6-13 - Embedded Creation, Last Access, and Last Write Times of Cheetos.jpg

Use the DCode tool to decode the embedded time stamps. You should have the following time stamps:

Embedded Creation Time (UTC): Wed, 18 December 2013 19:36:22 UTC

Embedded Access Time (UTC): Fri, 20 December 2013 08:00:00 UTC

Embedded Last Write Time (UTC): Mon, 14 January 2013 01:42:34 UTC

Note: You can tell a device is FAT32 based on the Last Access Time embedded in the link file. FAT32 does not track the time of the last accessed activity, only the date. In, DCode is reporting a last accessed date of 12/20/2013 and the time is 8:00 AM (UTC). DCode is attempting to report UTC by adding 8 hours to a field that by default reports 12:00 AM.

Next, take a look at the time stamps of the link file itself.

Figure 6-14 - Date and Time Stamps of the Link File

The link file's Modified date and time is different from the Created date and time. This means that Craig opened the file more than once.

Here is a timeline for the file "Cheetos.jpg" (All UTC):
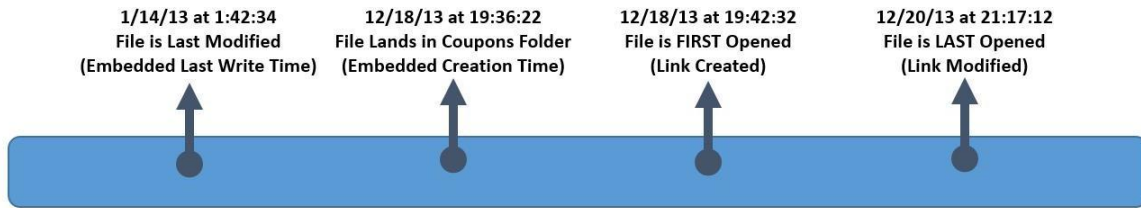
Figure 6-15 - Timeline of Cheetos.jpg Based on Link File

If a file has been opened more than two times, you will only know the FIRST time it was opened (Link Created) and the LAST time it was opened (Link Modified). Without other information, you will not know what the date and time stamps were when it was opened in between. The computer does not track the times in between,

Example 3 (No Embedded Date/Time)

Another example you will want to look at is the MileyCyrus_tongue.lnk. If you look at the link file in Hex view, you will see that there aren't any date and time stamps embedded in the link file.

Figure 6-16 - No Embedded Time Stamps in Link File for MileyCyrus_tongue.jpg

There are a few situations that can cause this to occur. If the user uses the function "Save as" on a picture when viewing a site using Internet Explorer, a link file will be created with no embedded date and time stamps. Once the user opens the file, embedded date and time stamps will be added in the link file. A link file is also created when a user does a "Save Image as" in Mozilla Firefox and Google Chrome. If the file isn't opened after it has been saved, there won't be any embedded date and time stamps as well.

With certain applications, if the user creates a file in an application and saves it, but never opens it, there won't be any embedded date and time stamps. Once they do open the file, embedded date and time stamps will be added to the link file.

If a user saves an email attachment but does not open it, there will be a link file with no embedded date and time stamps. This only applies to certain email client software programs, such as Windows Live Mail. Once the user actually opens the file, embedded date and time stamps will be added.

The Created time stamp of the link file shows when the picture was saved or created in an application. The Modified time stamp matches the Created time stamp because it was never opened.

If the file had been opened after it was saved, it would create date and time stamps embedded within the link file. The link file's Modified time stamp would show when the file was LAST opened.

So, if a link file has no embedded date and time stamps it means the user could have:

1) Used Save as on a picture in a website, but never opened the file
2) Created the file in an application, but never opened it
3) Saved an attachment through an email client software, but never opened the file

A link file with no embedded date and time stamps merely gives you an idea of where the file might have come from. Later, you will go through the user's email and Internet history. If you see the file as an email attachment or in their download history, you will know exactly where it came from.

Example 4 (File is Moved, Link File is Updated)

Now that you have an understanding of link files, let's take a look at how these can help in an investigation. Look at the link file called Underage_lolita_r@ygold_001.lnk and click on the Results view.

Figure 6-17 – Path of Underage_lolita_r@ygold_001.jpg

This link file shows that when the picture was opened, it was located in:

```
C:\Users\Craig\Pictures
```

If you go to that location, you will see that the picture is no longer there. Go back to the link file and look at the date and time stamps embedded in the link file.

Figure 6-18 - Embedded Creation, Last Access, and Last Write Times of Underage_lolita_r@ygold_001.jpg

Use the DCode tool to decode the embedded time stamps. You should have the following time stamps:

Embedded Creation Time (UTC): Sat, 21 December 2013 19:32:57 UTC

Embedded Access Time (UTC): Sat, 21 December 2013 19:32:57 UTC

Embedded Last Write Time (UTC): Sat, 21 December 2013 05:50:16 UTC

Next, take a look at the date and time stamps of the link file itself.

Figure 6-19 - Date and Time Stamps of the Link File

The link file's Modified date and time is different from the Created date and time. This means that Craig opened the file more than once.

Here is a timeline for the file "Underage_lolita_r@ygold_001.jpg" (All UTC):

12/21/13 at 5:50:16
File is Last Modified
(Embedded Last Write Time)

12/21/13 at 19:32:38
File is FIRST Opened
(Link Created)

12/21/13 at 19:32:57
File Lands in Pictures Folder
(Embedded Creation Time)

12/21/13 at 19:33:05
File is LAST Opened
(Link Modified)
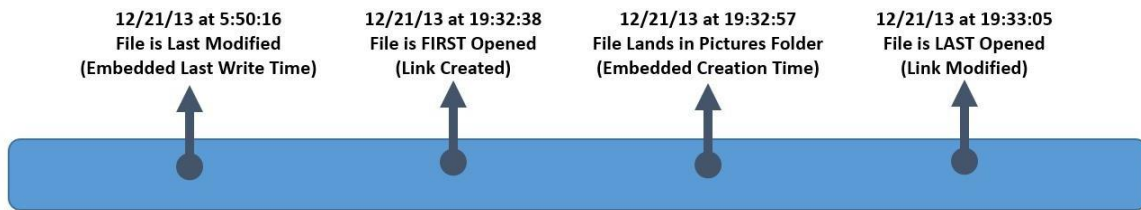
Figure 6-20 - Timeline of Underage_lolita_r@ygold_001.jpg Based on Link File

The embedded Last Write Time tells us that the file was last modified BEFORE the creation time. This indicates that the embedded Creation Time was when the picture was copied, not when it was actually created.

The link file was FIRST opened several seconds before the embedded Creation Time, which means it could have been opened on external media or in another folder before it was copied over.

When a file is opened in one location, it creates a link file. This is important to note that if a suspect then copies that same file to a different location and opens it there, a new link file is not created. The original link file is merely updated.

In this case, a link file was first created for the underage picture when it was opened in another location. When it was copied and opened in the Pictures folder, that same link file's embedded data was updated. The local path displays where it was last opened, and its embedded Creation Time is updated to when the file was copied to the Pictures folder.

You were able to determine the picture was opened somewhere else because the FIRST time it was opened was before the embedded Creation Time. In the next section, you will learn how jump lists can sometimes show other locations a file was opened in.

Note: This type of file naming is an indicator of child pornography. Searching for child pornography on this suspect's computer would be out of the scope of your original search warrant, which was just to search for coupons. In a normal investigation, you should obtain another search warrant to further investigate and see if the suspect had child pornography.

Jump Lists

Jump Lists were a new feature added to Windows 7. They are similar to the Windows shortcuts (link files) because they are designed to take a user directly to a specific file or directory used frequently or recently.
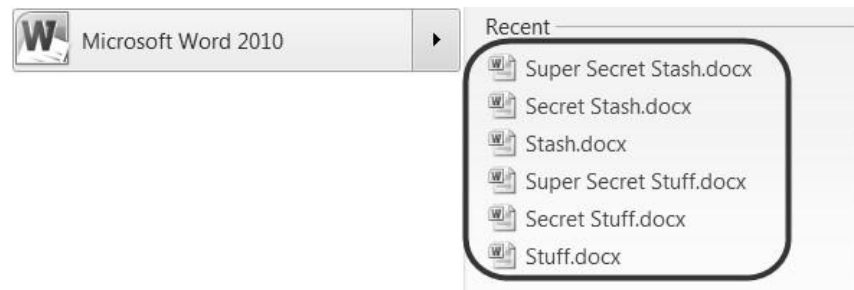

Figure 6-21 - Jump List for Microsoft Word

Jump lists are important to look at because they may contain information of file activity that is no longer present in the link files. However, you may also find file activity in link files but not in a jump list. It is important to note that these are two separate artifacts and will not always match up.

There are two sets of jump lists, which are called Destination files:

automaticDestinations, which are created and maintained by the operating system.

customDestinations, which are maintained by the specific application.

A jump list is basically a catalog of one or more link files associated with a specific application. This catalog stores the data in compound file binary (CFB) format. The jump lists are located in the following subdirectories for all versions of Windows:

```
C:\[username]\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
C:\[username]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations
```

There are various tools that you can use to review the contents of these files:

```
JumpLister from WoanWare: https://github.com/woanware/JumpLister
Windows Jump List Parser from TZWorks: http://www.tzworks.net
```

For this case, use JumpLister from WoanWare. To use this tool you need to first export the jump lists. Navigate to the folder in the Tucker image that contains them.

Each jump list file name starts with a hex value prefix. This prefix is the Application ID. A resource for looking up AppID's is located at:

```
http://forensicswiki.org/wiki/List_of_Jump_List_IDs
```

Go ahead and highlight all the jump list files in the AutomaticDestinations folder, right-click one, and select Extract File(s) (see Figure 6-22).
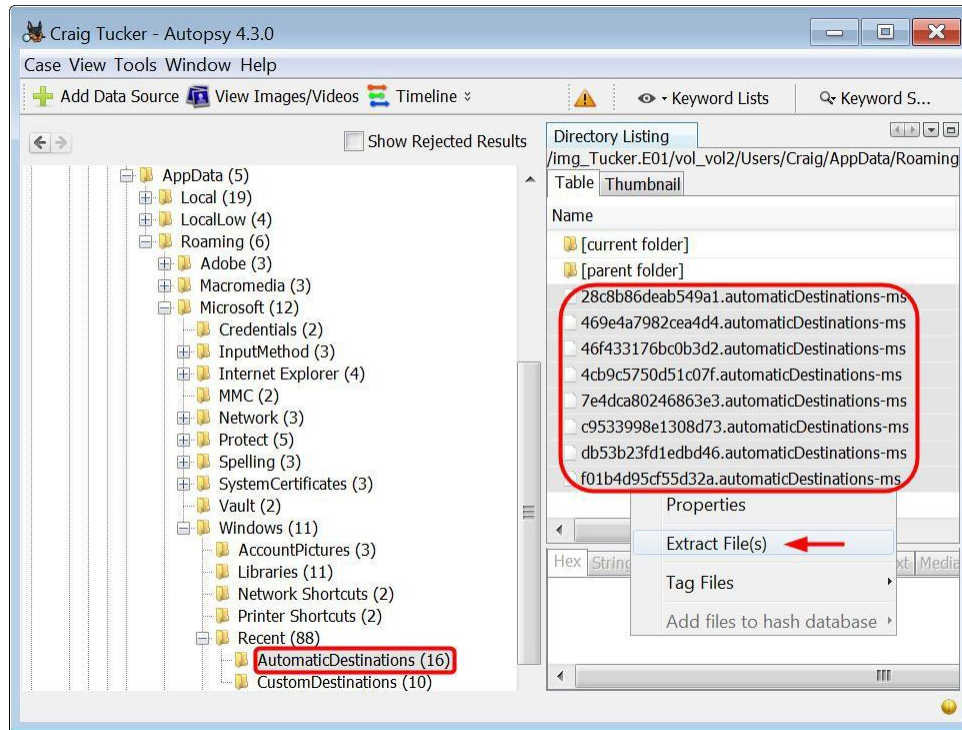
Figure 6-22 – Highlight Jump Lists in AutomaticDestinations, Right-Click and Select Extract File(s)

Extract these files to your case Export folder. Open up the JumpLister tool where you downloaded it, and then select File►Load.
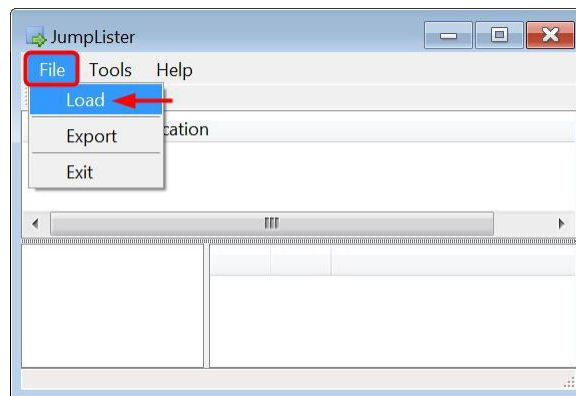
Figure 6-23 – Click Load in JumpLister

Navigate to your export folder that contains the jump list files. Highlight and select each jump list file and click Open.

If you click the jump list 46507-c9533998e1308d73.automaticDestinations-ms in JumpLister, you can see what pictures have been opened (see Figure 6-24).
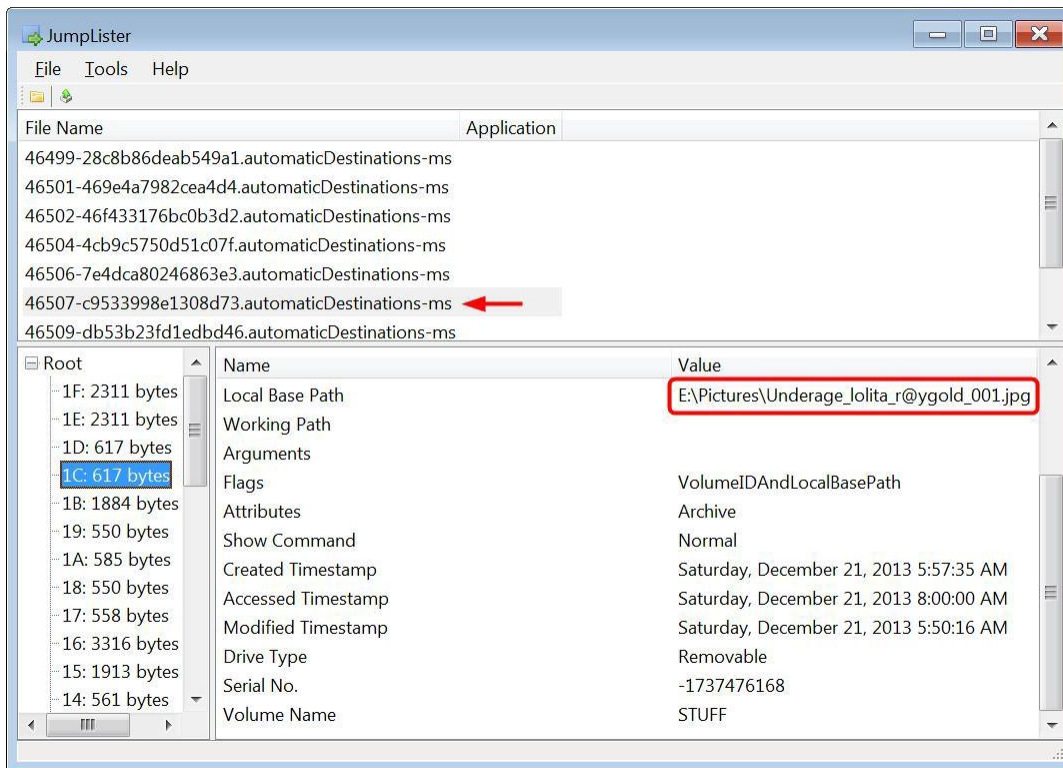
Figure 6-24 - Individual Entries in Photos App Jump List

Note: This version of Jumplister does not display what application goes with the jump list c9533998e1308d73. This application is the Windows 8 "Photos" app and it is the default photo viewer in Windows 8. This application is also present in Windows 10.

In the bottom left pane, there are entries for individual files that have been opened. These entries are equivalent to a link file because they show where the file was located and it has the embedded date and time stamps.

The bottom left pane also has an entry called DestList (Destination List). This list is a summary of each entry (see Figure 6-25). There are three key fields that you want to focus your attention:

Number: This number will be associated with the entry number in the bottom left pane

Date/Time: This is the last time the file was accessed with the program

Data: This is the file location and filename
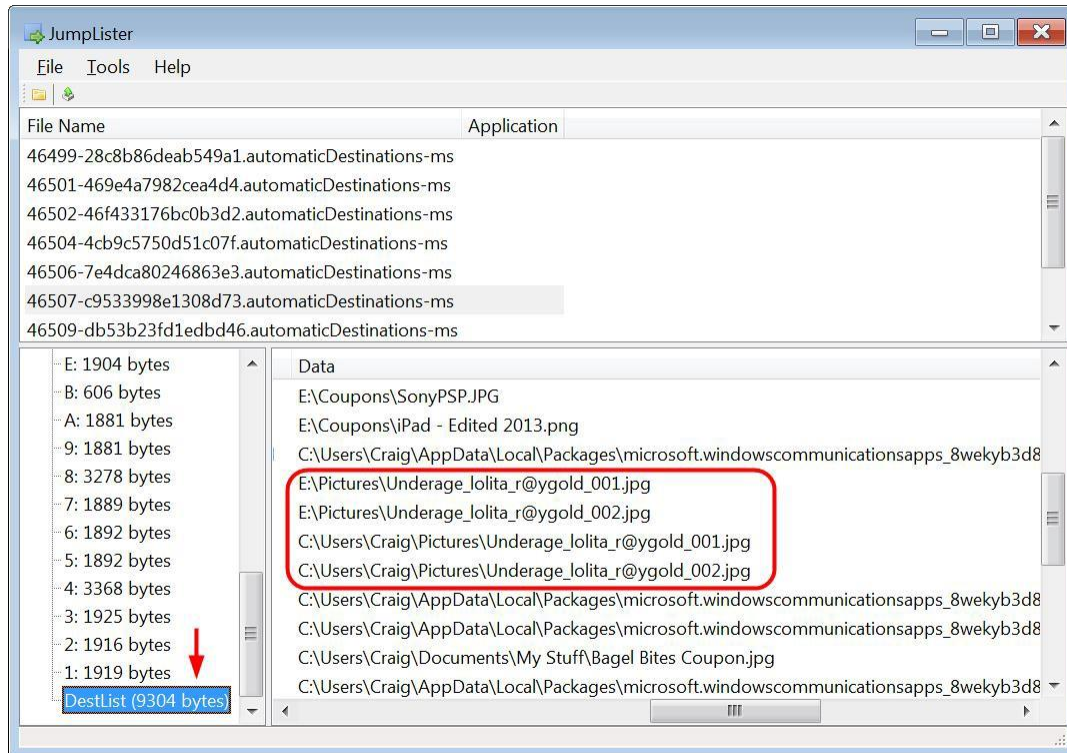
Figure 6-25 - DestList in Jumplister

As you can see in Figure 6-25, the jump list shows the underage pictures that were opened on the E: drive. You did not have this information in the link files because the link files were updated.

You can see in the column Date/Time that the pictures Underage_lolita_r@ygold_001.jpg and Underage_lolita_r@ygold_002.jpg were opened on the E:\ drive and in the Pictures folder on the following dates:

Underage_lolita_r@ygold_001.jpg (E: Drive):	12/21/13 7:32:38 PM (UTC)
Underage_lolita_r@ygold_002.jpg (E: Drive):	12/21/13 7:32:45 PM (UTC)
Underage_lolita_r@ygold_001.jpg (Pictures Folder):	12/21/13 7:33:05 PM (UTC)
Underage_lolita_r@ygold_002.jpg (Pictures Folder):	12/21/13 7:33:10 PM (UTC)

Note: There are two other timestamps called Timestamp (New) and Timestamp (Birth). These are related to Object IDs, which is a more advanced topic. For now, just use the Date/Time stamp to determine when the file was first opened.

You can export out this jump list information to a CSV file by clicking File►Export
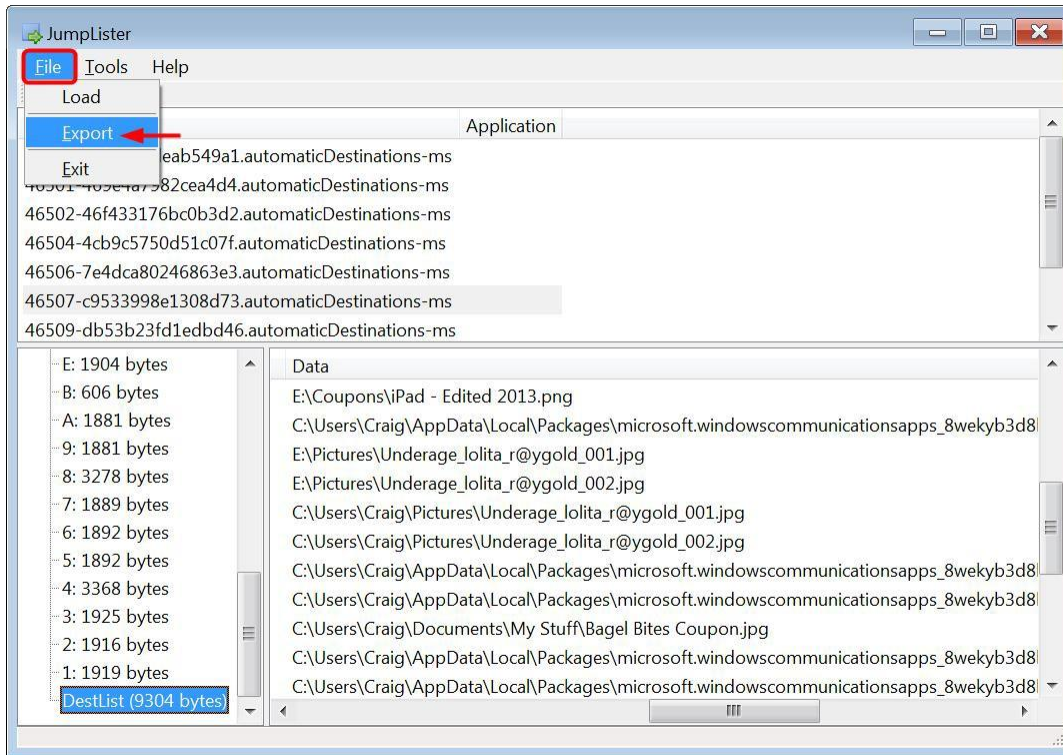
Figure 6-26 - Export Jump List Information to CSV File

Export the files to your case's Export Folder. Now, open up Excel and go to the Data tab. Click "From Text" under "Get External Data".
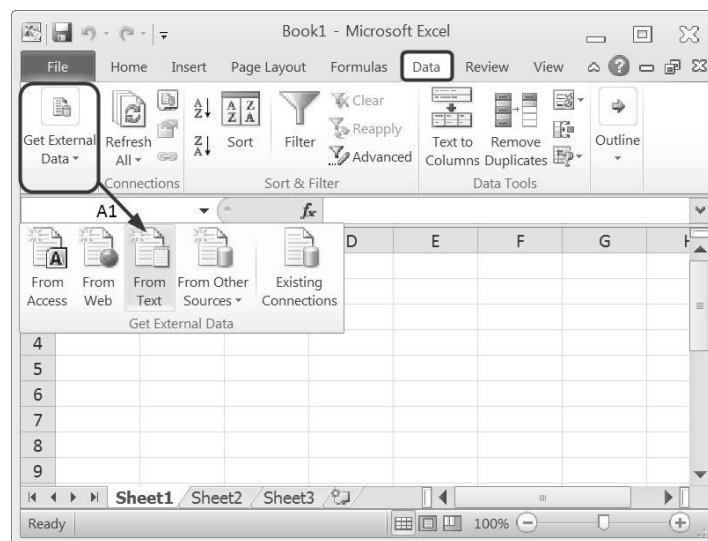
Figure 6-27 - Get External Data from Text to Open CSV File

Navigate to your Tucker Export\Jumplist folder and open the file DestList.csv. A window will open and prompt you to choose your text import options. Pick Delimited and click Next (see Figure 6-28).
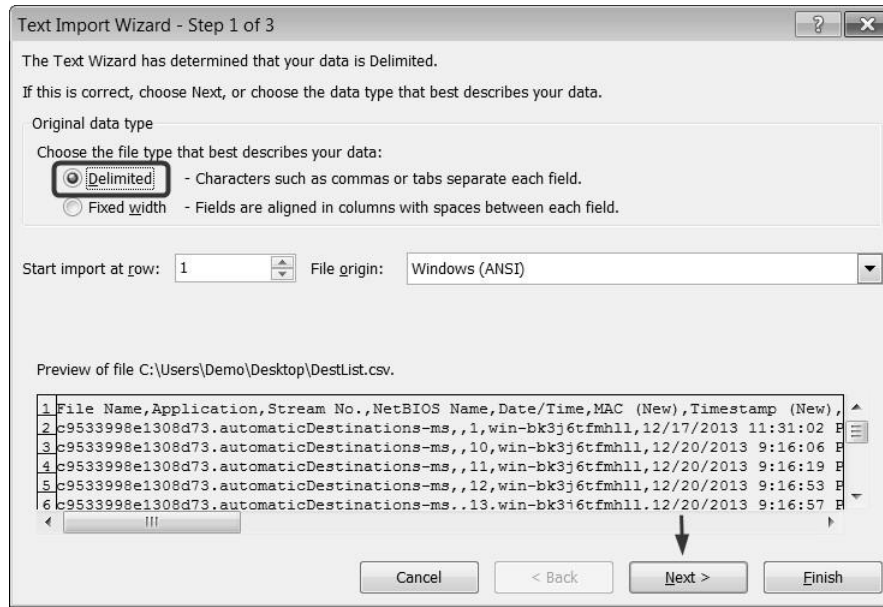
Figure 6-28 - Import DestList.csv as Delimited

Check the Comma delimiter and hit Finish.
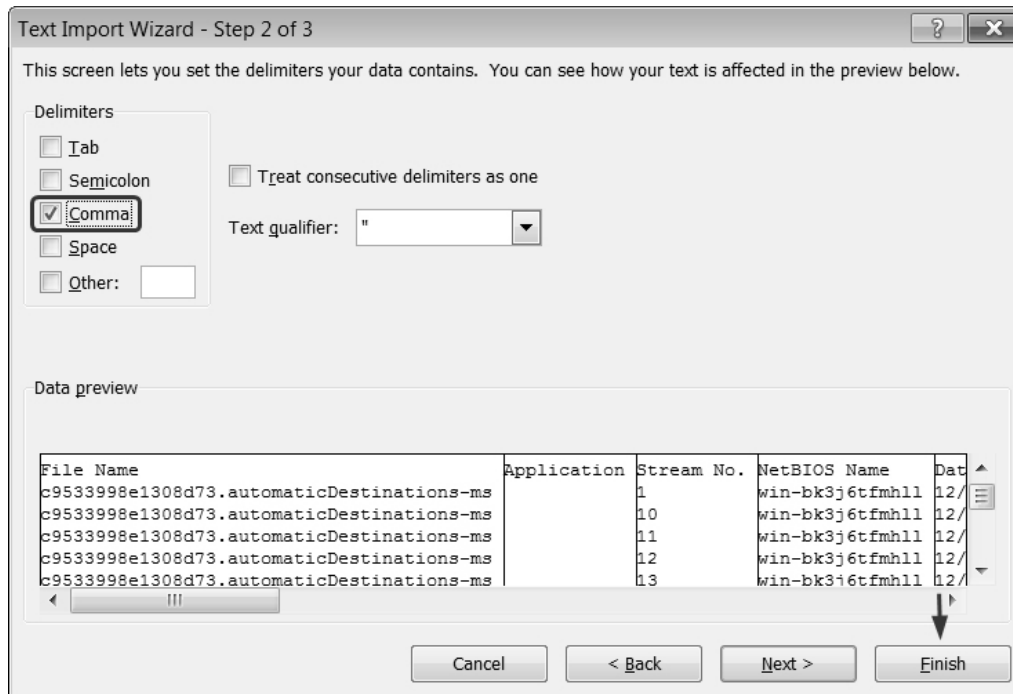
Figure 6-29 - Set Comma as Delimiter

This will give you a clean report of the jump list information (see Figure 6-30).

File Name	Date/Time	Data
c9533998e1308d73.automaticDestinations-ms	12/17/2013 23:31	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscom
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\desk_setup.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\School\SMC_Library.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\Santa Monica\Park.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\Santa Monica\Pier.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:17	E:\Coupons\Coca- Cola.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:26	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscom
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:28	C:\Users\Craig\Documents\Guides\HowtoMakeCoupons.jpg
c9533998e1308d73.automaticDestinations-ms	12/21/2013 0:55	E:\Coupons\GiftCards.jpg

Figure 6-30 - CSV of Jump List Information

If you click on one of the cells in the top row and then click the Filter button under the Data tab, you can easily filter for specific text or sort the columns.
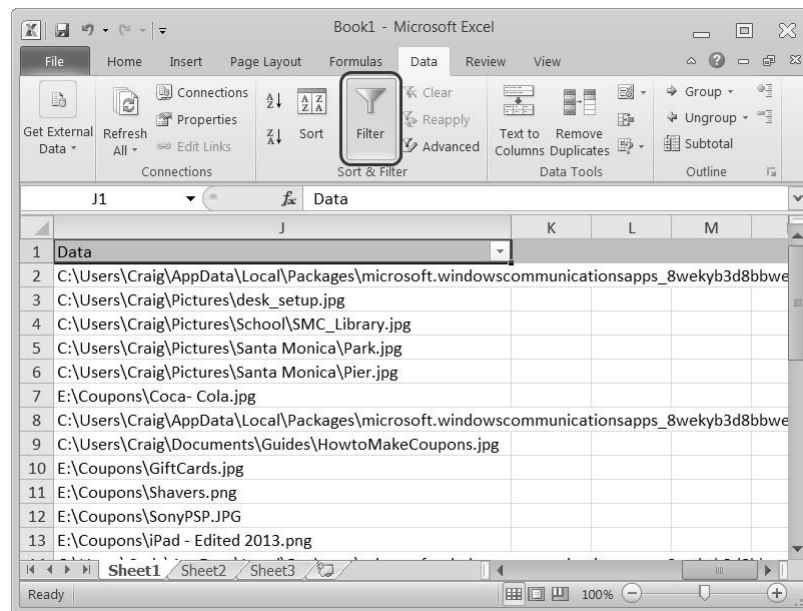
Figure 6-31 - Filter Function in Excel under Data Tab

By clicking the arrow at the end of each column header, you can select filters such as Text Filters►Begins With. These are helpful if you want to only view files on external media or just on the C: drive.
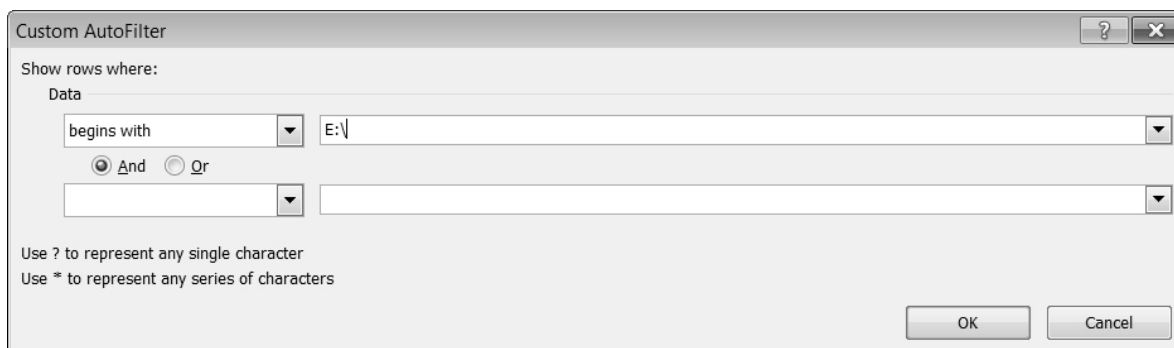
Figure 6-32 - Text Filter Begins with E:

CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 7: Recycle Bin

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

7

Recycle Bin

Introduction

Since the file "Underage_lolita_r@ygold_001.jpg is no longer in the Pictures folder and you don't have Craig's E: drive, you should see if it was deleted. Most computer users believe that when a file is deleted and the recycling bin is emptied, that the file cannot be accessed. However, deleting a file can still leave data behind for recovery. This is because when a file is deleted, the data is only marked as deleted by the computer and allows that area of the disk to be available for storing new data. It's not until the user overwrites this area of the disk that the data is actually deleted. Even part of the original file may still be recoverable if the user only overwrote a portion of the disk space. Therefore, this data can be recovered by investigators. This process is known as "file carving."

$R and $I Files

The first time a user deletes a file, the file is not actually deleted. A new folder is created in the Recycle Bin, and the deleted files are moved to it. The folder that is created is named after the security identifier (SID) and the relative ID (RID) of the associated user. You can use this information to determine which user account deleted the file. You are going to look at Craig's Recycle Bin (see Figure 7-1), which is located in:

```
C:\$Recycle.Bin\S-1-5-21-1049150138-4017234595-3791460656-1001
```
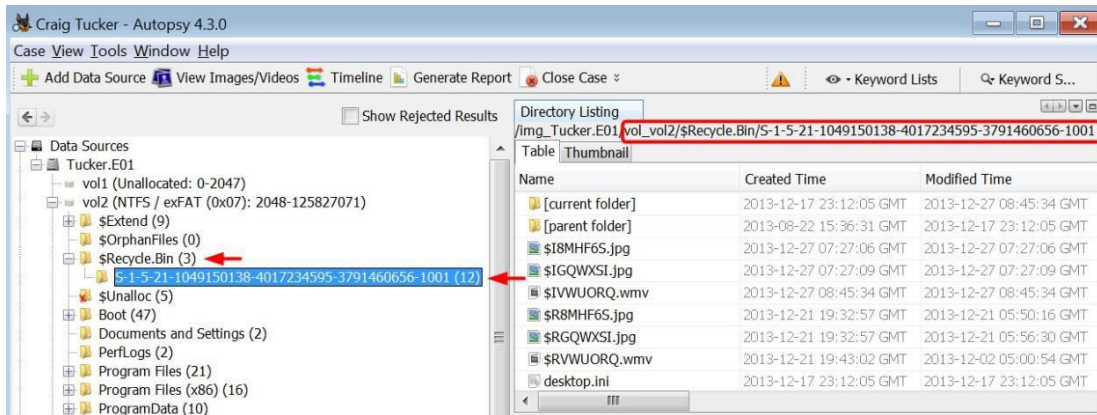
Figure 7-1 - Craig's Recycle Bin

Note: If a user deletes a file using the command prompt or does Shift+Del, the file bypasses the Recycle Bin and it is deleted right away.

Both file names contain 6 identical, random characters and its original extension, preceded by either $I or $R. The **$I** file contains information about the deleted file including the file's size, deleted time, path, etc. The **$R** file contains the actual deleted file itself.
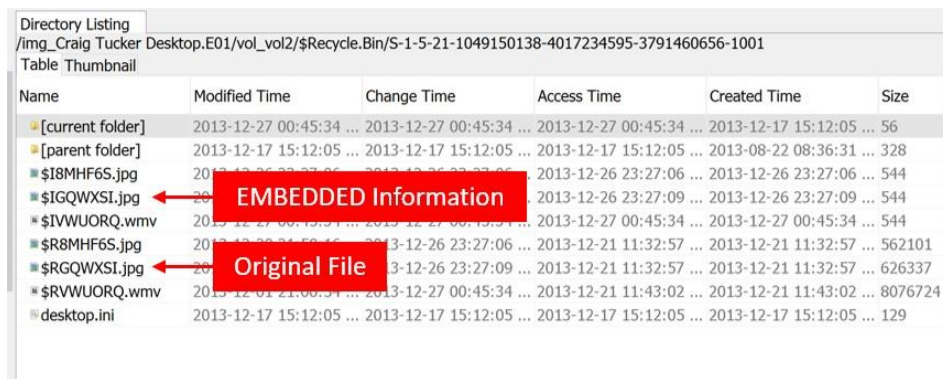
Figure 7-2 - $I and $R Files

In Autopsy, look at the $I file called $IGQWXSI.jpg and click the Strings view. You will see the path of where $IGQWXSI.jpg was originally stored on the computer before the user deleted the file.
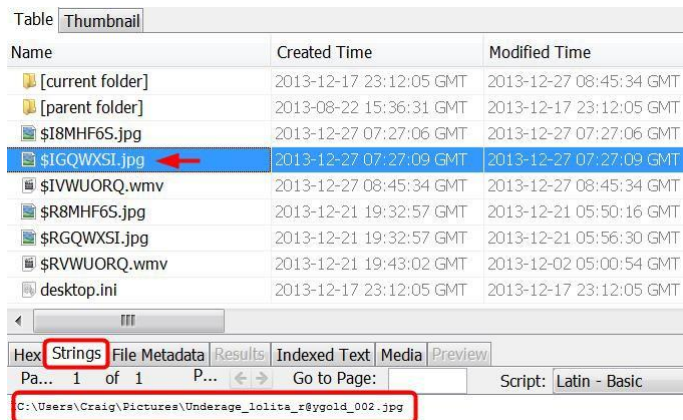
Figure 7-3 - $IGQWXSI File Shows Location and Name of File Before Deletion

Next, if you view $IGQWXSI.jpg in Hex view, you can see there is EMBEDDED data regarding the file before it was deleted. There are three pieces of critical information: the Windows version, file size, and time and date.
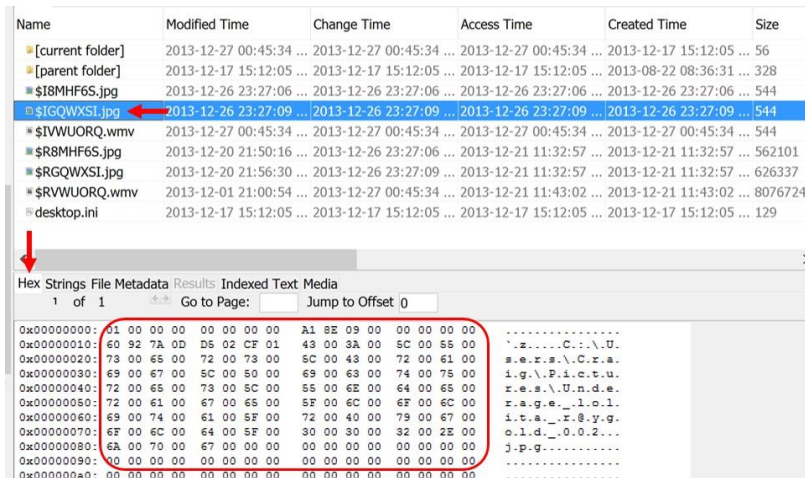
Figure 7-4 – Embedded Data in $IGQWXSI File

The first 8 bytes of the $I file tell you the Windows version the file was created on. If the first byte is "01" then the user's computer was running Windows 8 and "02" if the user was running Windows 10. The second set of 8 bytes (starting at offset 8) represent the size of the original file.
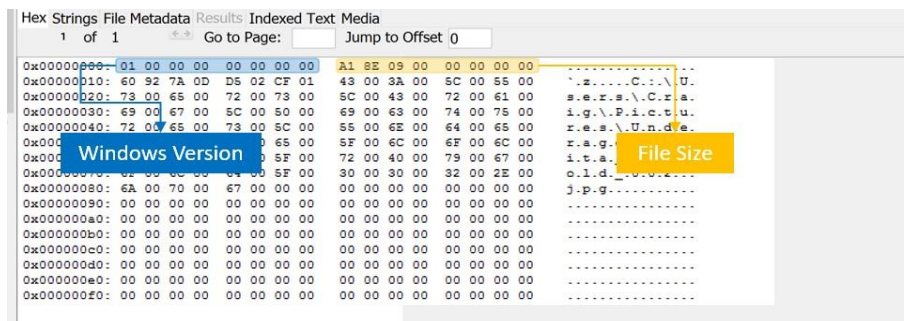
Figure 7-5 – Embedded Information on Windows Version and Size of File

The hex value of the file size is represented in "Little Endian" format which means the little end is read first. To convert this into human-readable information you must read the hex value with the larger order first (read the sets of two digits from right to left). Therefore, you would convert from "Little Endian" as follows:
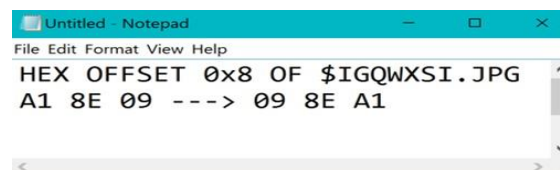
Figure 7-6 – Convert Little Endian Format by Reading Data Right to Left

Then convert this hex value to a decimal to get the file size in bytes by using a conversion calculator. To do so, you are going to use the following website:

```
http://www.rapidtables.com/convert/number/hex-to-decimal.htm
```

Once you have this calculator open, type your converted human-readable hex value into the "Enter hex number" box and then click "Convert".

Figure 7-7 – Type in Converted File Size Hex Value from $$IGQWXSI.jpg and Click Convert

The value displayed in the "Decimal number" box in the conversion calculator is the size of the file before it was deleted by the user in bytes.

Next, encoded in the hex value of $IGQWXSI.jpg is the date and time stamp of when the file was deleted.

Figure 7-8 – Embedded Deleted Time Stamp in $IGQWXSI.jpg

To decode the timestamp, you are going to once again use the DCode (Version 4.02a) tool. Once you have DCode open, you need to copy the time stamp from the Hex tab of the selected $I file which begins at offset 16 and is 8 bytes in length. Then, set the Decode Format to Windows: 64 bit Hex Value - Little Endian. Click the Decode button to see the decoded Date and Time. You should have Fri, 27 December 2013 07:27:06 UTC for when the file Underage_lolita_r@ygold_002.jpg was deleted from the user's Pictures folder (see Figure 7-9).
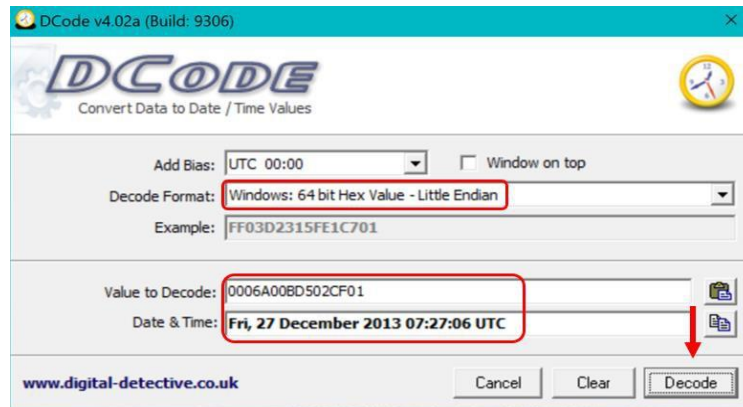
Figure 7-9 – Copy Deleted Time Stamp, Set Format to Little Endian, and Click Decode

Note: This encoded date is important to decode since Autopsy does not automatically provide the Deleted time in its platform. This often helps with creating timelines in analysis.

Now, look at the file called $RGQWXSI.jpg and click on Media view. You will see a preview of the file that was deleted by the user. In this case, you should see a .jpg picture.
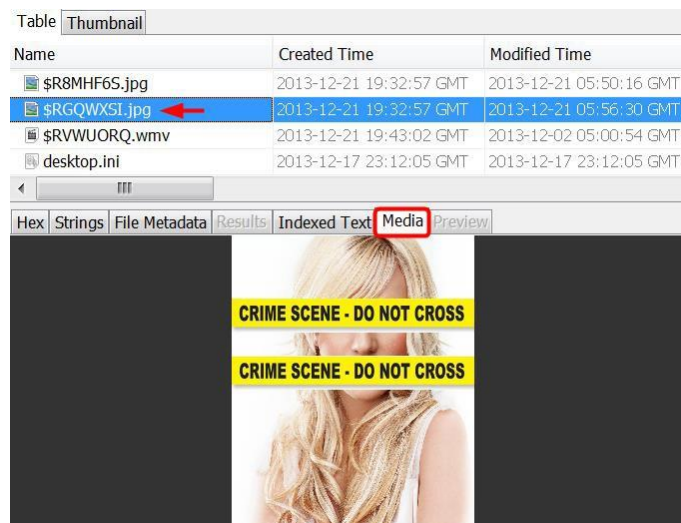

Figure 7-10 – Preview $RGQWXSI.jpg with Media View

Note: Throughout these practice and test images, you may see pictures with crime scene tape. These are the simulated child pornography images, and you should tag any of these images since they are important to your investigation.

CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 8: External Storage Devices

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

8

External Storage Devices

Introduction

When you looked at Craig's link files and jump lists, some of the data was pointing to an E: drive, which was a removable disk. These link files pointed back to potential fraudulent coupons and CP. Now that you are aware of the suspect's external E: drive, you need to know more about it. It is also important for you to learn more about USB devices and what information is stored when they are plugged into a computer.

USB devices are designed under USB Bus specifications, which describe the design and technical details for manufacturing them. From a forensics viewpoint, there are a couple of technical details under the Standard USB Descriptors Definitions that help to identify a specific USB device. Each USB device contains information that is embedded at the time of manufacturing.

You can use a freeware tool, such as Microsoft's Universal Serial Bus Viewer (USBView) to read the information. USBView can list USB host controllers, USB hubs, and attached USB devices. The following information for a SanDisk, U3 Cruzer Micro, 2GB thumb drive was extracted using USBView:

```
===>Device Descriptor<===

bLength:                0x12
bDescriptorType:        0x01
bcdUSB:                 0x0200
bDeviceClass:           0x00->This is an Interface Class Defined Device
bDeviceSubClass:        0x00
bDeviceProtocol:        0x00
bMaxPacketSize0:        0x40 = (64) Bytes
idVendor:               0x0781 = SanDisk Corporation
idProduct:              0x5406
bcdDevice:              0x0200
iManufacturer:          0x01
English (United States) "SanDisk"
iProduct:               0x02
English (United States) "U3 Cruzer Micro"
iSerialNumber:      0x03
English (United States) "43174013F2C14667"
bNumConfigurations:     0x01
```

The key fields of information that can be relevant to a forensic investigation are:

Vendor ID (idVendor)

Product ID (idProduct)

Manufacturer (iManufacturer)

Product (iProduct)

Serial Number (iSerialNumber)

Since I physically possessed the device, I could confirm the accuracy of the information listed by USBView. I could see that the device was in fact a SanDisk U3 Cruzer Micro. However, the serial number was not stamped on the exterior of the device. You should also be aware that while some devices may have a serial number that is visible, it may not match the serial number that is embedded in the USB circuit board.

No matter what serial number is stamped on the exterior, you will always want to check the internal serial number, which is also called the iSerialNumber.

The Vendor ID, which is 2 bytes in length, is assigned by the USB Implementers Forum, Inc. Each vendor is assigned a unique ID.

The Product ID is also 2 bytes in length, but it is randomly assigned by the manufacturer. A good reference for Vendor and Product ID's can be found at the following website:

```
http://www.linux-usb.org/usb.ids
```

Although the information on this website shouldn't be considered authoritative, since it's submitted by individuals, it is a good starting point to look up information that may match the Product ID.

Another freeware tool that can be used to read a USB device is USBDeview, which can be downloaded from:

```
http://www.nirsoft.net
```
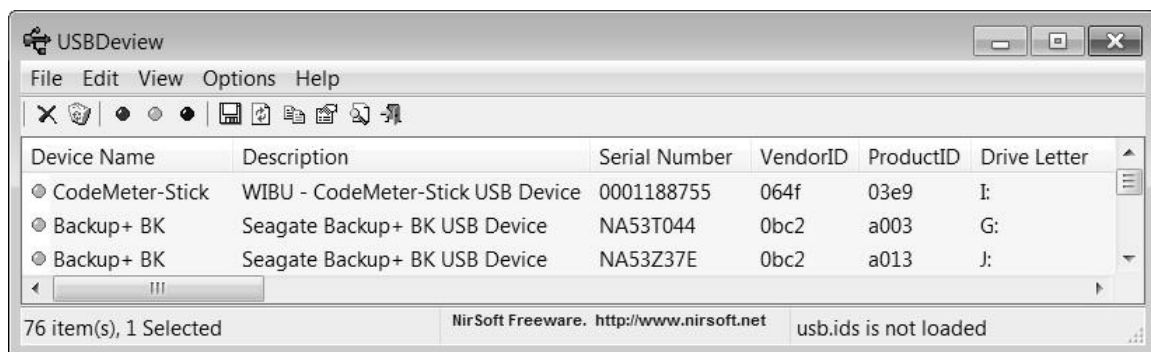

Figure 8-1 – USBDeview

Windows Plug and Play

Now that you know what information is embedded in a USB device, you need to understand what happens when a USB device is plugged into a Windows-based computer.

The plug and play manager extracts information from the USB device when it is first plugged into a Windows computer. As you can see in Figure 8-2, it records that information in several locations.
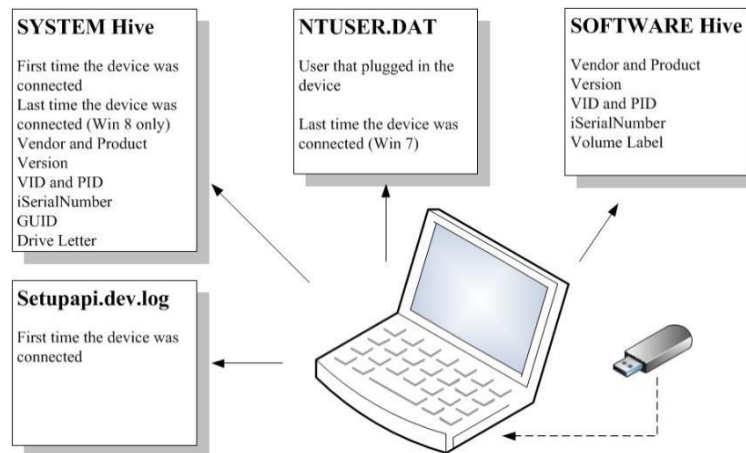
Figure 8-2 - Information Recorded when USB is Connected

Autopsy Devices Attached

When you ran modules earlier on Autopsy, it pulled different information from the registry, including devices connected.
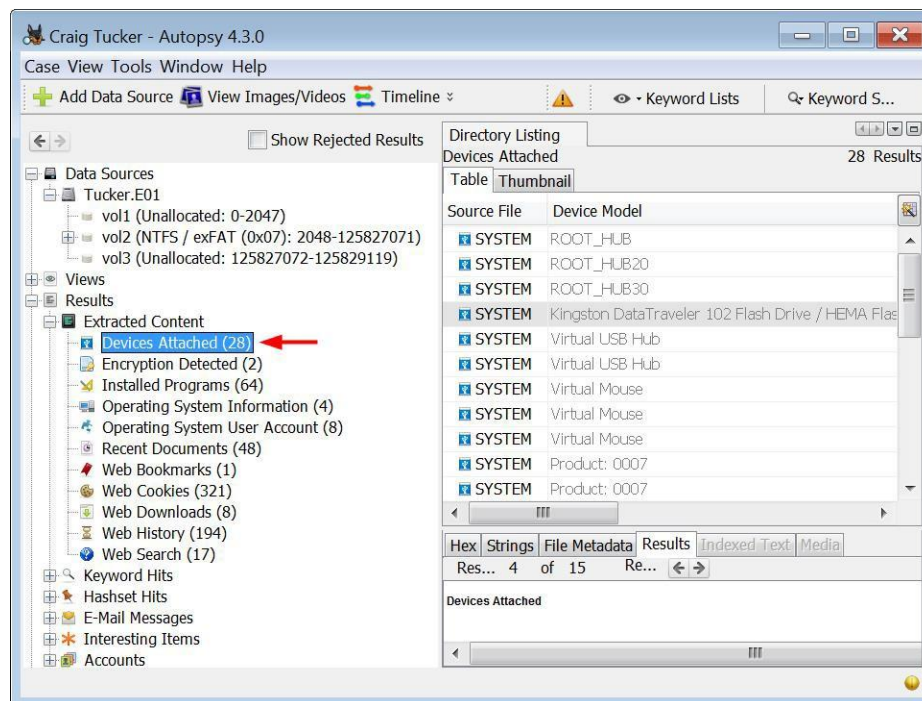
Figure 8-3 – Devices Attached Information Autopsy Retrieved After Running Module

While this information can be useful at face value, it does not really give much detail on the devices actually connected. There are also entries that are not related to external drives that were physically connected, which is not useful to the investigation at the moment. You are going to extract the four key files that store USB information (SYSTEM, SOFTWARE, NTUSER.DAT, and setupapi.dev.log) and then use another tool to find more detailed information.

SYSTEM Hive

Throughout these next sections, you can use the Windows 8 USB Worksheet in the Appendix to follow along with the useful information you want to find for connected USBs.

When a USB device is first connected, it stores the following information in the SYSTEM hive:

Vendor

Product

Version

VID and PID

iSerialNumber

GUID

Drive letter of the USB

Open the SYSTEM hive in Registry Explorer and navigate to the following subkey:

    [CurrentControlSet]\Enum\USBSTOR

Note: As you may remember from earlier, the Select subkey showed you that the current control set was 1. In this case, it is also the only control set in this SYSTEM hive.
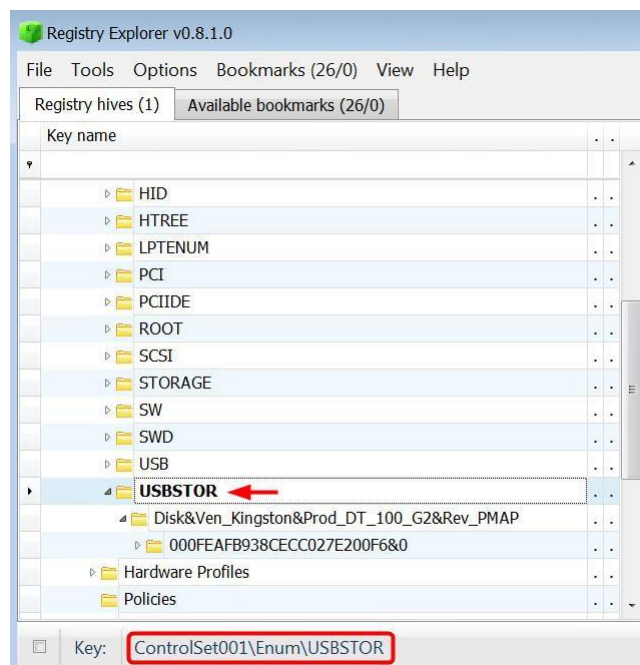
Figure 8-4 - USBSTOR Subkey in SYSTEM Hive

You will see a subkey under USBSTOR which has a name with the following information:

Vendor (Ven):   Kingston

Product (Prod):   DT_100_G2

Version (Rev):   PMAP

✔**Checkpoint:** Write Vendor, Product, and Version in Section 1 on your USB worksheet.

Below this subkey is another subkey named after the iSerialNumber "000FEAFB938CECC027E200F6&0", which Microsoft calls the Instance ID. By omitting the suffix (&#), you can see the iSerialNumber.

Note: The (&#) suffix shows what port the USB device was connected to.

✔**Checkpoint:** Write the iSerialNumber in Section 2 on your USB worksheet.

Open up the iSerialNumber subkey and go to the following location:

```
Properties\{83da6326-97a6-4088-9453-a1923f573b29}
```

As you can see in Figure 8-5, this subkey contains six subkeys. Four of the subkeys, 0064, 0065, 0066, and 0067, have important time stamps. The subkey 0064 shows the date and time when the device's driver was first installed. The subkey 0065 shows when the device's driver was installed. 0064 and 0065 will typically be the same date and time.

The subkeys 0066 and 0067 are new to Windows 8. 0066 shows when the device was last connected and 0067 shows when the device was last removed.
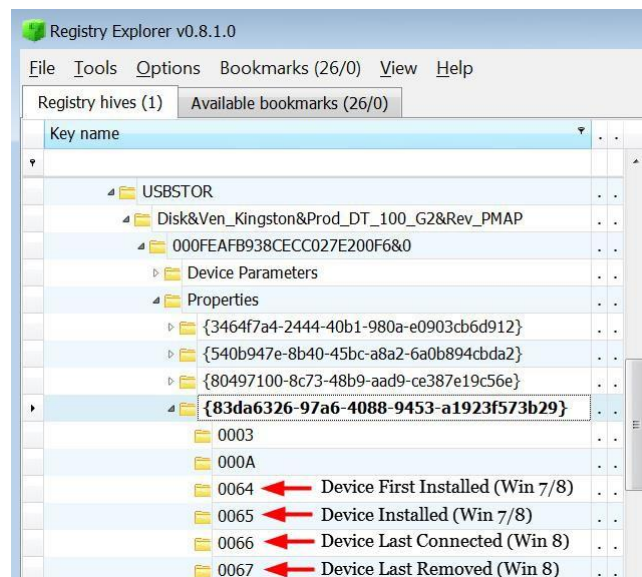
Figure 8-5 - Date and Time Stamps for USB Device

✔**Checkpoint:** Write the first time connected, last time connected, and last time removed in Sections 3, 4, and 5 on your USB worksheet.
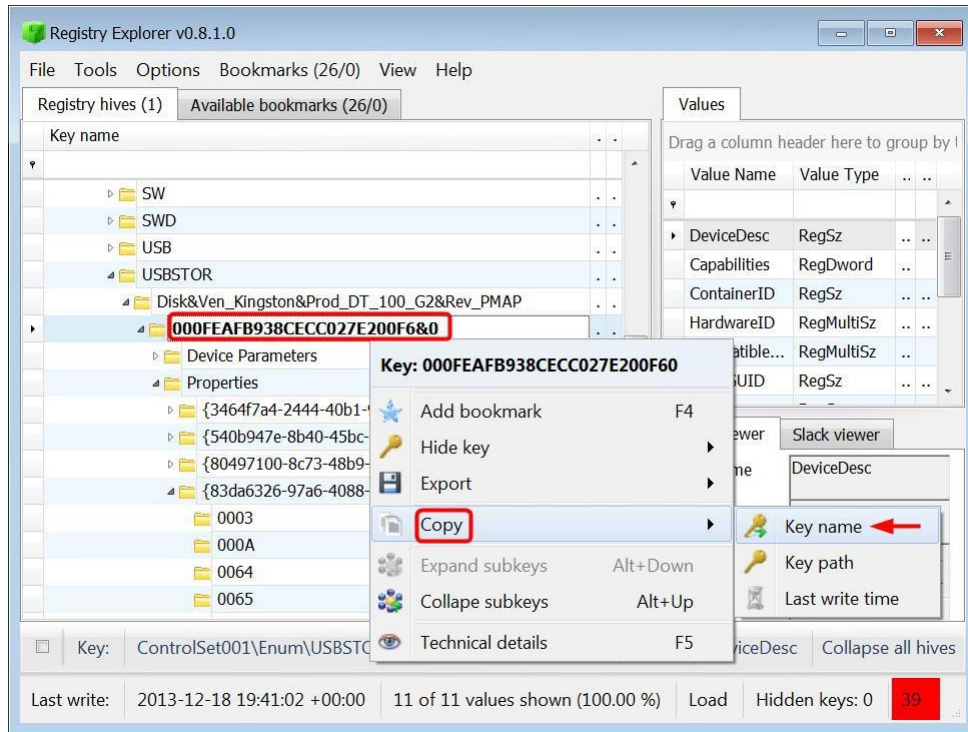
Figure 8-6 – Right-Click iSerialNumber Subkey and Select Copy Key Name

Press Control+F or click on Tools►Find to conduct a search. When the Find window opens, paste the iSerialNumber into the Search For field. Delete the &0 at the end of the iSerialNumber. Check Key Name, Value Data, and Value Name. Leave Value Slack unchecked and then click Search.
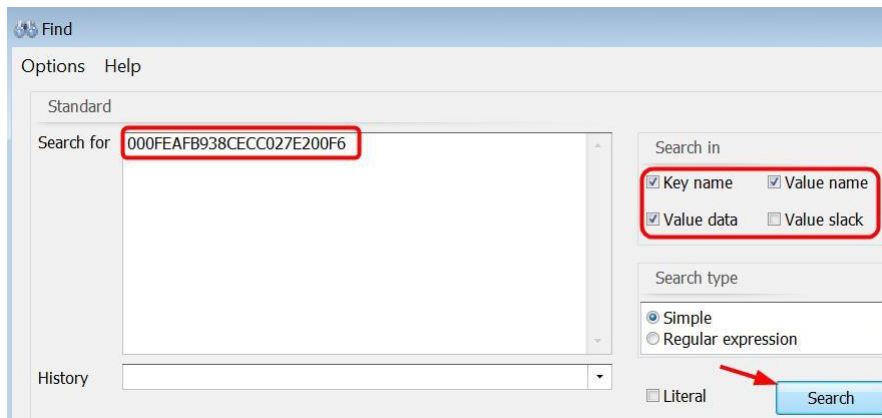
Figure 8-7 – Paste iSerialNumber, Check Key Name/Value Name/Value Data, Click Search

Down in the results pane, you want to look in the Key Path column for a hit under the USB subkey and the Mounted Devices subkey.
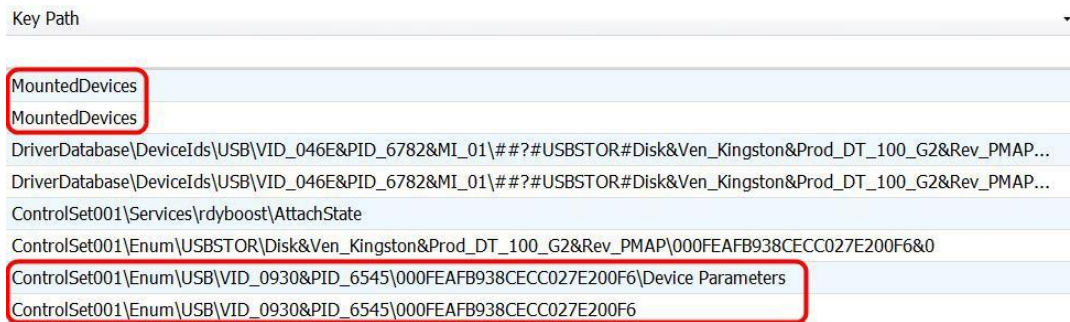
Figure 8-8 – Search Result in MountedDevices and USB Subkeys

First, the iSerialNumber for the connected Kingston device is under the USB subkey. The iSerialNumber has a parent subkey named with the Vendor ID (VID) and the Product ID (PID), which in this case is "VID_0930&PID_6545".

✔**Checkpoint:** Write the VID and PID in Section 6 on your USB worksheet.

Close out of the Find window and navigate to the MountedDevices subkey. Take a look at the different values in the MountedDevices subkey. There are two types of values here. There are some values with names of GUIDs and some values with drive letter names. The value named "Volume{16d5eeec-681c-11e3-824f-000c29d6ef92}" contains information on the Kingston USB. A GUID is a 16-byte value that is randomly generated. Since the value consists of 128 bits, it is unlikely that a randomly generated GUID will match another GUID.
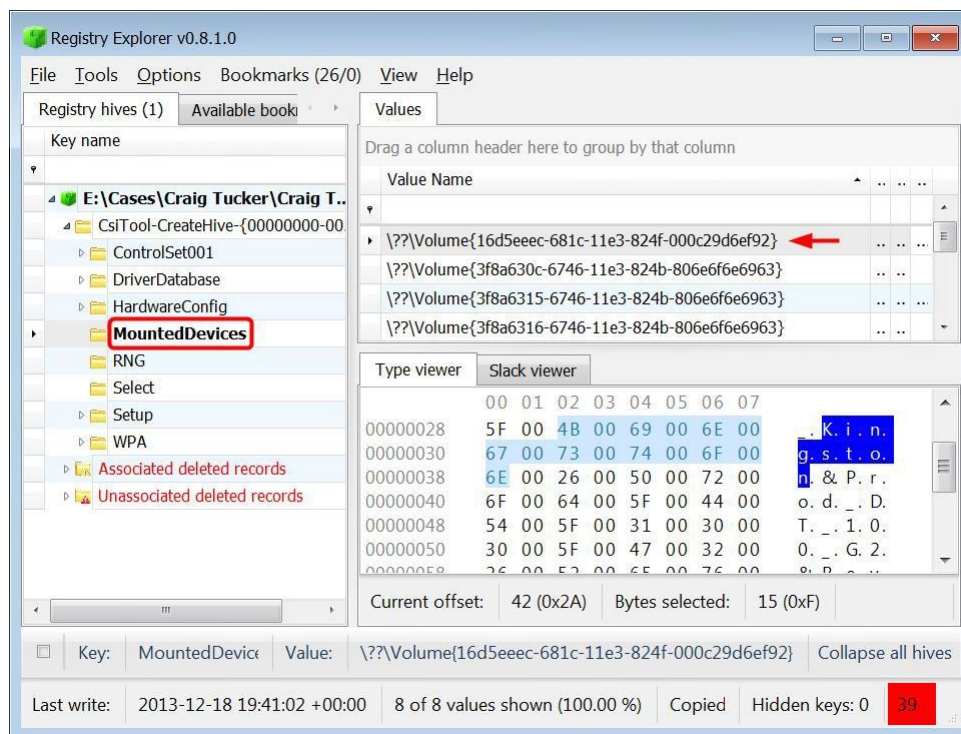
Figure 8-9 – Kingston UBS Information in GUID Value

✔**Checkpoint:** Write the GUID in Sections 7 on your USB worksheet.

Next take a look at the drive letter values. If you look at the value "DosDevices\E:", you will see Kingston USB information in it. This device's drive letter is E. If the drive letter had been assigned to another drive that was attached at a later date, the drive letter information would be overwritten with the new device's serial number.
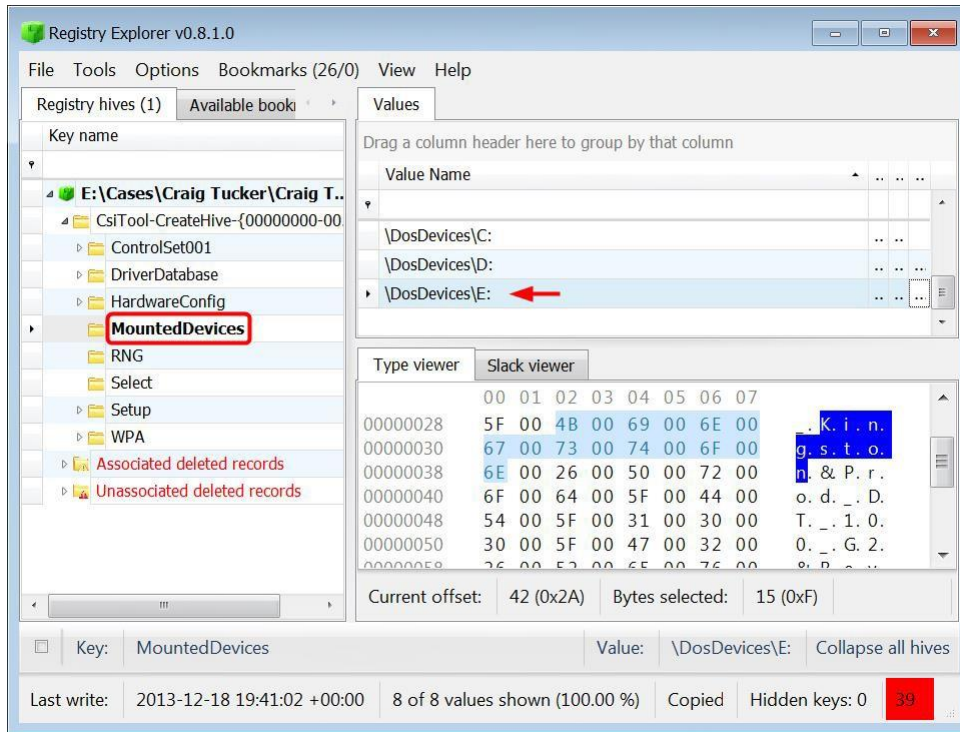
Figure 8-10 – Kingston USB Information in E: Drive Letter Value

✔**Checkpoint:** Write the Drive Letter in Section 8 on your USB worksheet.

SOFTWARE Hive

When a USB device is connected, it stores similar information in the SOFTWARE hive. However, one important piece of information that is only in the SOFTWARE hive is the Volume Label. Open the SOFTWARE hive with Registry Explorer and navigate to the following subkey:

```
Microsoft\Windows Portable Devices\Devices
```

There is only one subkey below Devices, since only one device was connected. The subkey name will contain the same information you found in the SYSTEM hive, except it doesn't have the GUID and drive letter. The subkey will also have a value name called "FriendlyName". The value data of FriendlyName contains the Volume Label, which is "Stuff".
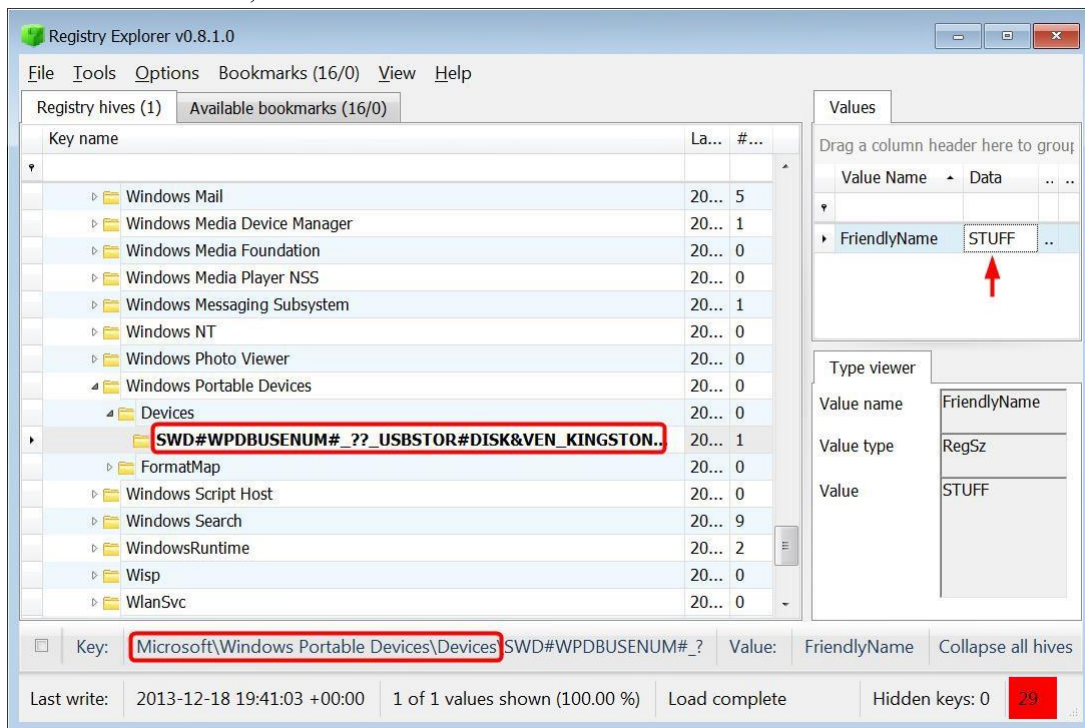
Figure 8-11 - Volume Label in SOFTWARE Hive

✓**Checkpoint:** Write the Volume Label in Section 9 on your USB worksheet.

If you remember from the Recent Files section, a link file stores the volume label and volume serial number where the file was located.

The volume serial number is created when the device is formatted. The way it is calculated is based on the date and time of when the device was formatted, which means that the chance of two devices having the same volume serial number is very unlikely.

A device's volume label can be changed at any time, but the volume serial number can only be changed if the device is reformatted.

NTUSER.DAT

If the computer contained multiple user accounts, you would want to know which user plugged in the device. The user profile hive (NTUSER.DAT) will show you if that user account was specifically associated with that USB device. It will also show you the last time the device was plugged in by that user.

Open Craig's NTUSER.DAT file in Registry Explorer and conduct a search in the NTUSER.DAT file for the first part of the device's GUID (16d5eeec) that you obtained earlier. Only have Key Name checked and then click Search.

Note: Make sure you remove other hives from Registry Explorer before conducting a search so your results will only come from the NTUSER.DAT file.
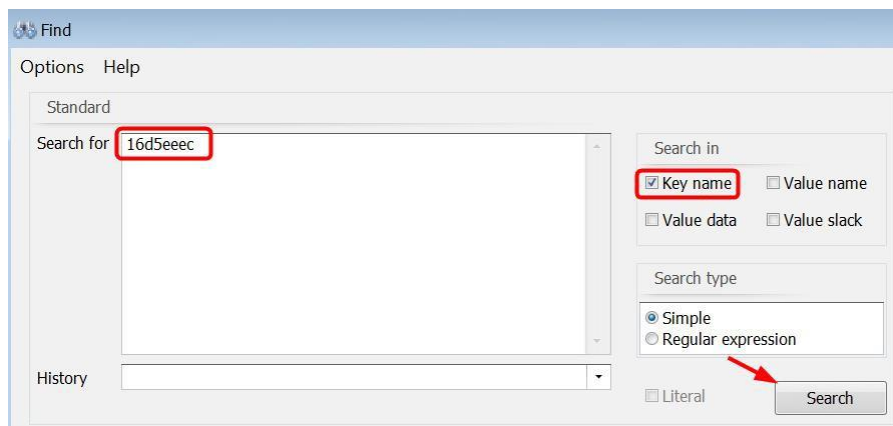
Figure 8-12 – Search for First Part of GUID in Craig's NTUSER.DAT File and Click Search

You should see a result in the following subkey:

Key Path

Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{16d5eeec-681c-11e3-824f-000c29d6ef92}
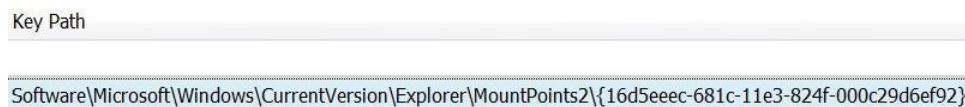
Figure 8-13 – Search Result of Kingston USB GUID

Since the device's GUID is located in Craig's NTUSER.DAT under the MountPoints2 subkey, you know that he was the user that plugged in the device.

✔**Checkpoint:** Write the user that connected the device in Section 10 on your USB worksheet.

Note: Since you do not have the subkeys 0066 and 0067 in the SYSTEM hive for Windows 7 machines, you could look at these Key Properties to determine the last time the device was connected. However, you would not know the last time the device was removed.

Setupapi.dev.log

When a USB device is first connected, it also stores information in the "setupapi.dev.log" file. You already know the first time the device was connected from the SYSTEM hive, but this is another file that will show you the first time the USB device was connected. It is located in:

```
C:\Windows\inf
```
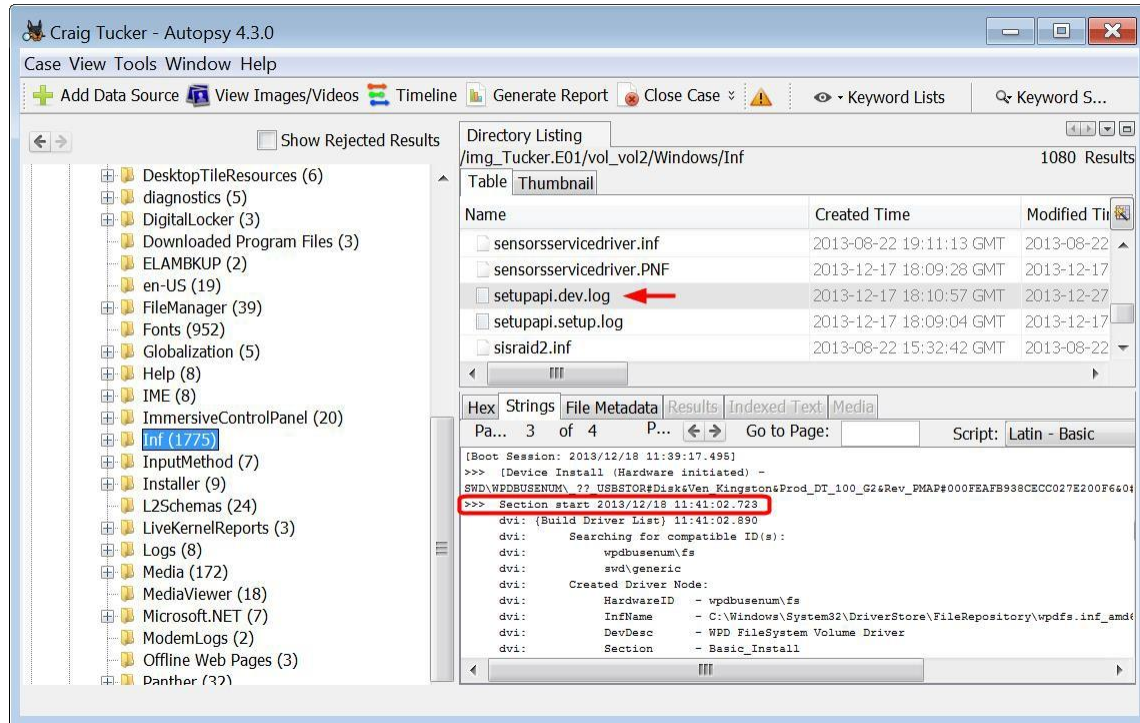
Figure 8-14 – Setupapi.dev.log File

If you click through the pages of the setupapi.dev.log file, you will find an entry for the Kingston USB with the following text:

```
>>>  [Device Install (Hardware initiated) -
SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP#000FE
AFB938CECC027E200F6&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
>>>  Section start 2013/12/18 11:41:02.723
```

The last line that starts with ">>> Section start" contains the date and time when the device was first connected. This log records information in local time. That means that the first time the device was plugged in was December 18, 2013 at 11:41 AM (PST).

You are going to need this file for the USB tool, so go ahead and extract the setupapi.dev.log file by right-clicking it and selecting Extract File(s) (see Figure 8-15).
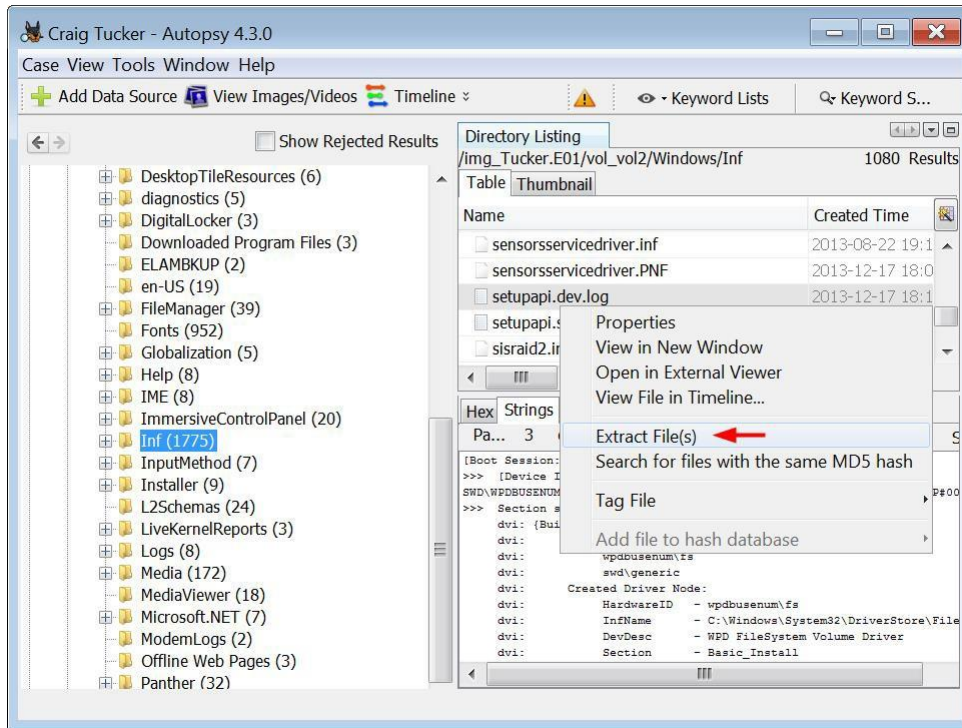
Figure 8-15 – Extract setupapi.dev.log to Export Folder

Navigate to the setupapi.dev.log file to the case Export folder and click Save.

USB Historian

Now that you know what information is stored when a USB device is connected, and where it is stored, you can use tools to quickly create a USB report. You are going to use a tool called USB Historian from 4Discovery, which you can download for free from their website:

```
https://4discovery.com/usb-historian/
```

Open the USB Historian tool, and in the top left corner you need to click the button Open File(s). A Wizard window will open, and you need to choose Select Individual Hives/Files. Click Next.
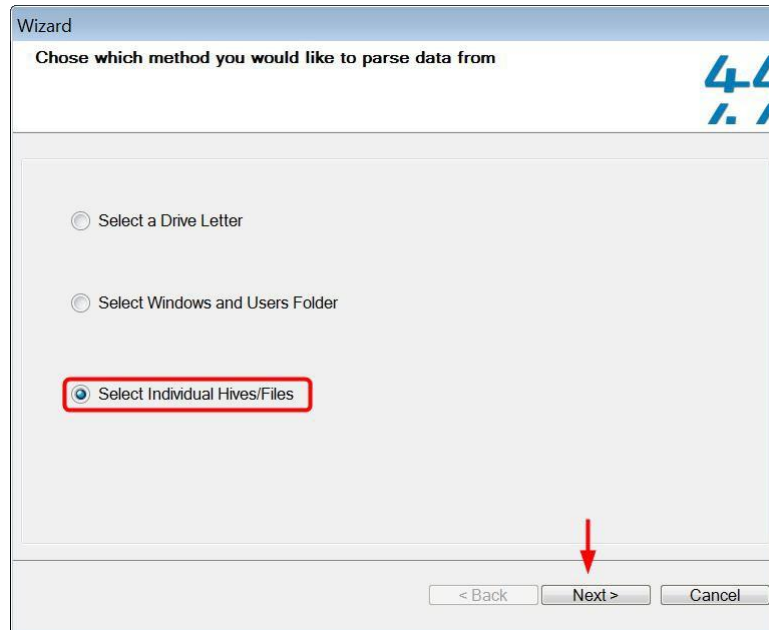
Figure 8-16 – Choose Select Individual Hives/Files and Click Next

When the next window opens, you need to add the SYSTEM hive, the SOFTWARE hive, the NTUSER.DAT registry hive, and the setupapi.dev.log file you exported. Navigate to your case's Export folder and add each corresponding hive or file and then click Finish (see Figure 8-17).
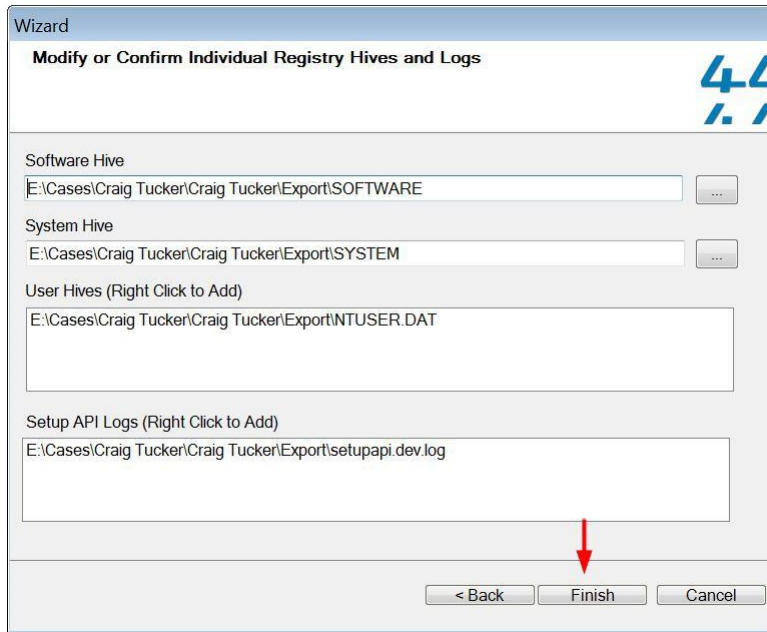
Figure 8-17 – Add Exported SOFTWARE, SYSTEM, NTUSER.DAT, setupapi.dev.log and Click Finish

Friendly Name	Serial No	S_	Mount Point 2	Drive Letter	Volume Name	Ready Boost Volume Name
Kingston DT 100 G2 USB Device	000FEAFB938CECC027E200F6		[Craig:12/21/2013 9:23:15 PM]	E:		STUFF

Friendly Name: The name of the device. (Found in SYSTEM hive)

Serial No: The iSerialNumber of the device. (Found in SYSTEM hive)

Mount Point 2:   The user that plugged in the device and the last time (UTC) that the device was plugged in by that user. (Found in NTUSER.DAT)

Vol: The device's drive letter. (Found in SYSTEM hive)

Ready Boost Volume Name: Volume label of the device. (Found in SOFTWARE hive)

Usb Stor DateTime	Usb Stor DateTime64	Usb Stor DateTime65	Vendor	Product	Version	Vid	Pid
12/18/2013 7:41:02 PM			Ven_Kingston	Prod_DT_100_	Rev_PMAP	VID_0930	PID_6545

Usb Stor DateTime   The date/time that the device driver was installed (Found in SYSTEM hive)

Vendor, Product, Version: The vendor, product, and version. (Found in SYSTEM hive)

Vid and Pid: The Vender ID and Product ID. (Found in SYSTEM hive)

Guid
16d5eeec-681c-11e3-824f-000c29d6ef92

Guid: The device's GUID. (Found in SYSTEM hive)

Computer Forensics CCIC Training

Chapter 9: Email

Lauren Pixley, Cassidy Elwell, and James Poirier

9

Email Review

Introduction

Email can become a vital part of your investigation. In this case, you are looking for fraudulent coupons and now there are issues with CP. It is important to check email, because you need to know who your suspect was communicating with and if they were trading any data. You know that there were fraudulent coupons and CP associated with a USB device, but could the suspect have also received this type of data from other people?

Suspects can use webmail or software such as Thunderbird or Outlook to view their mail. It can be difficult to sometimes recover any email if the user was just using webmail, since most of it is not stored on the computer itself. However, if the suspect uses software to view their mail, then you can typically see what emails or attachments they sent and received.

Windows 8 Mail App

In Autopsy, click on E-Mail Messages under Results in the left pane. As you can see, Autopsy is reporting that there are zero email messages.
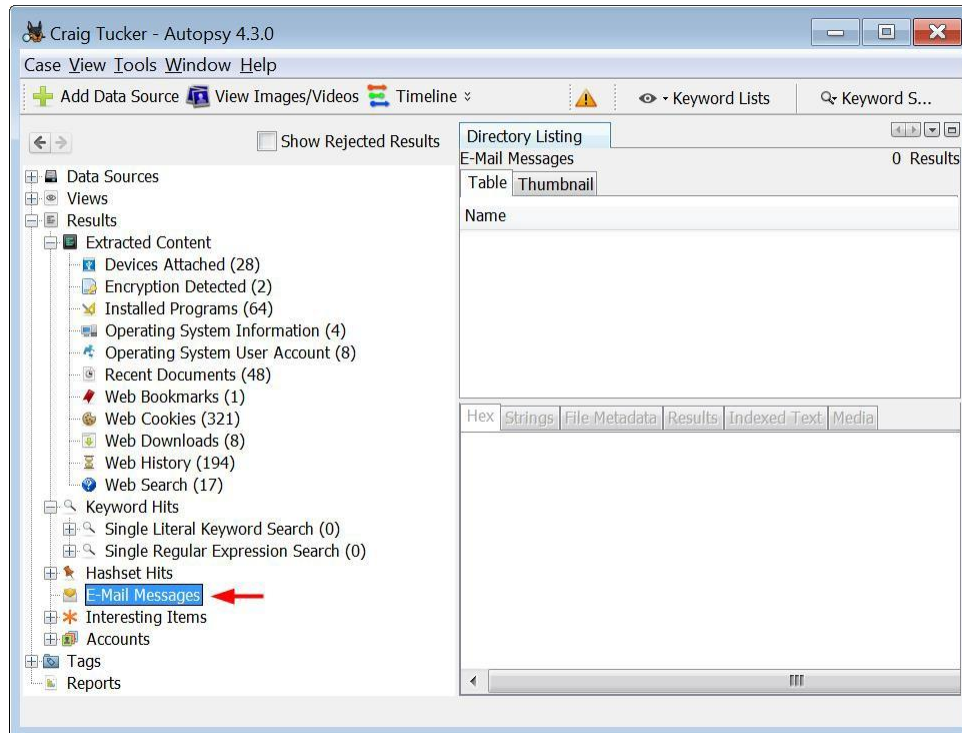
Figure 9-1 – Autopsy Shows Zero E-Mail Messages

Just because Autopsy shows zero email under this tab, that does not necessarily mean the suspect didn't have any email. They could have been using mail through their web browser or they could have been using a mail app that Autopsy does not recognize. You know that for this image, the suspect's operating system is Windows 8. That means the suspect could have been using the built-in Windows 8 Mail app, which is a program that Autopsy does not pull or recognize as email. To see if Craig used the Windows 8 Mail app, navigate to the following subfolder:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\Indexed\LiveComm\ba871ed4e8a350e0\120712-
0049\Mail\1
```

In a Windows 10 image, the path is slightly different to get to all the emails and the way they are stored is not the same as it was in Windows 8 and earlier. Now, they are stored as .dat files which can be opened through a web browser. This adds a level of security in Windows 10 for consumers, but makes your job as a forensic examiner more difficult. To see if Craig had used the Windows 10 Mail app, you would navigate to the following subfolder:

```
C:\Users\Craig\AppData\Local\Comms\Unistore\data/1/a
```
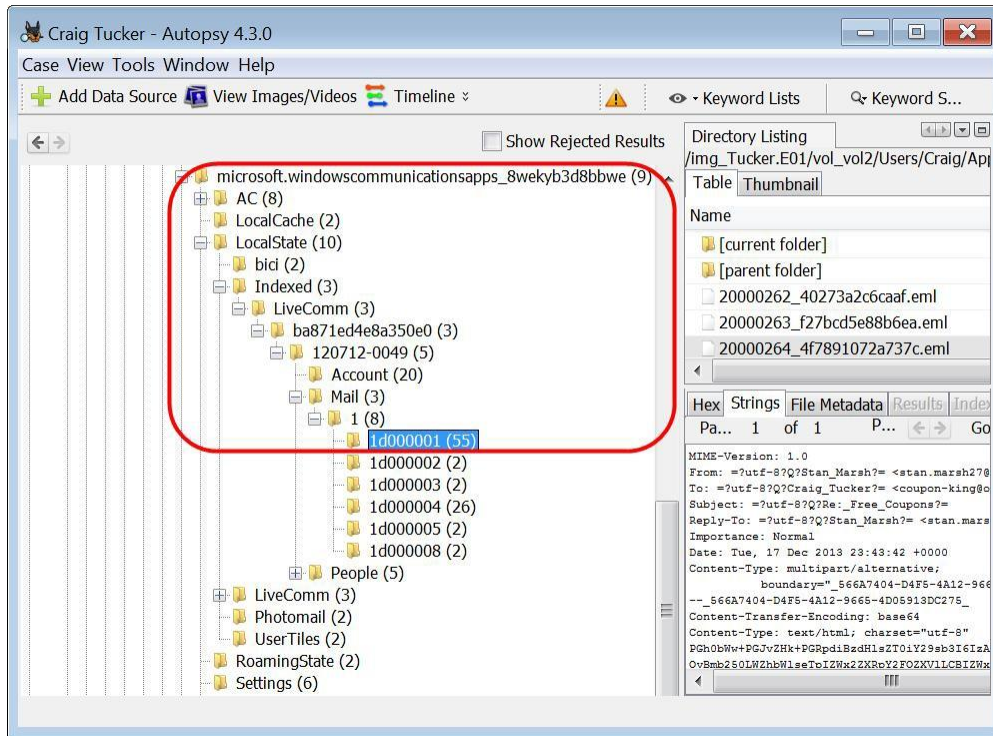
Figure 9-2 – Subfolders for Windows 8 Mail App

Below the Mail\1 subfolders, there are six subfolders. These subfolders that are named 1d00000# represent a mail folder, such as Inbox, Sent, Deleted. Take a look at the first eml file in the 1d000001 subfolder that has the subject "Free Coupons".
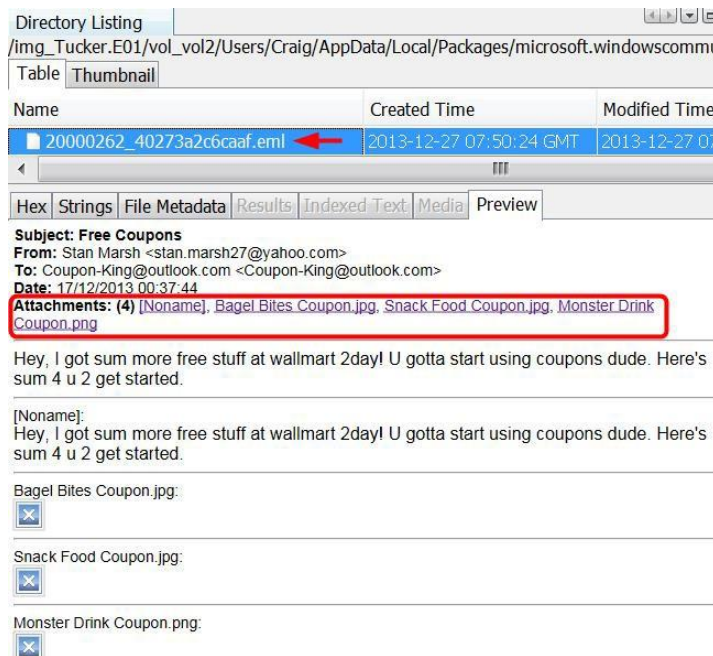
Figure 9-3 – Free Coupons Email in 1d000001 Subfolder

This email is from someone named Stan Marsh and they sent 3 attachments. Since this relates to your investigation, go ahead and tag the eml file with any tag name you prefer (see Figure 9-4).
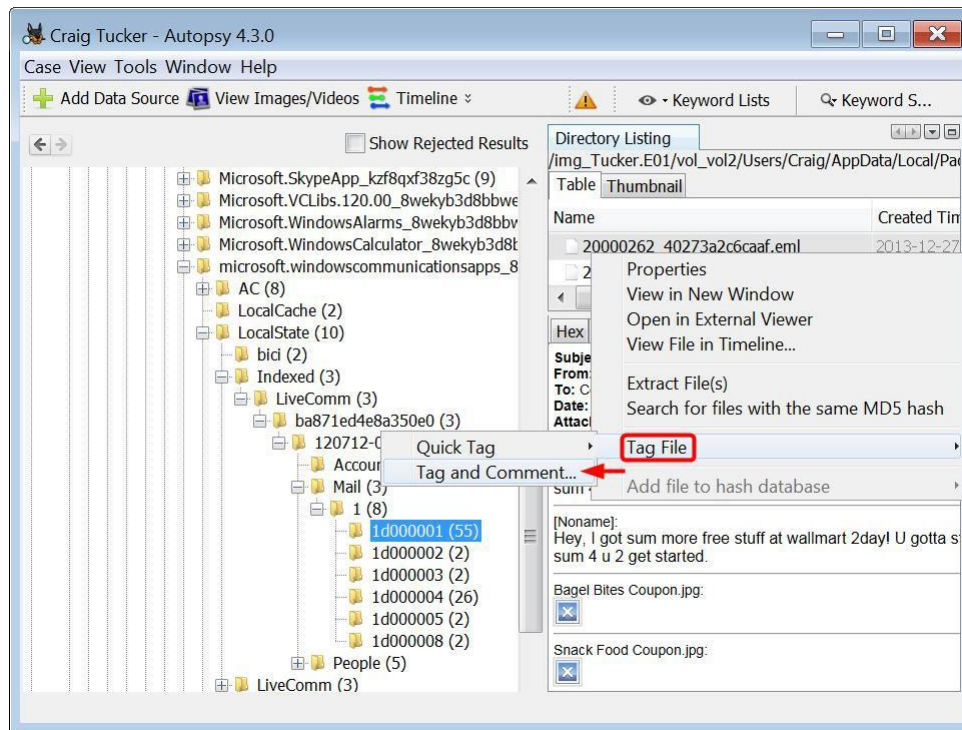
Figure 9-4 – Tag Free Coupons Email

Attachments

With Windows 8 mail, all of these emails are being stored in eml files. If you look at the line in the email called "Attachments", you will see the names of three jpgs attached to the email. With Windows 8 mail, the user has to download the attachments. Even when the attachments are downloaded, they are not encoded and stored in the same eml file as the email. If the user downloaded the attachment from mail, it is stored in an attachment folder called Att.

First, take a look at the eml file that this email is being stored in. One thing you should check before looking at the attachments folder is the first part of the eml name. This number is the Message ID and will match the email's attachment folder. Make note that the Free Coupons email attachment folder will be named 20000262. The attachment folder is located in:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\LiveComm\ba871ed4e8a350e0\120712-0049\Att
```

There are several subfolders below the Att folder, and their name matches up to an eml file name. Look for the subfolder 20000262. This contains the Free Coupons email attachments (see Figure 9-5).
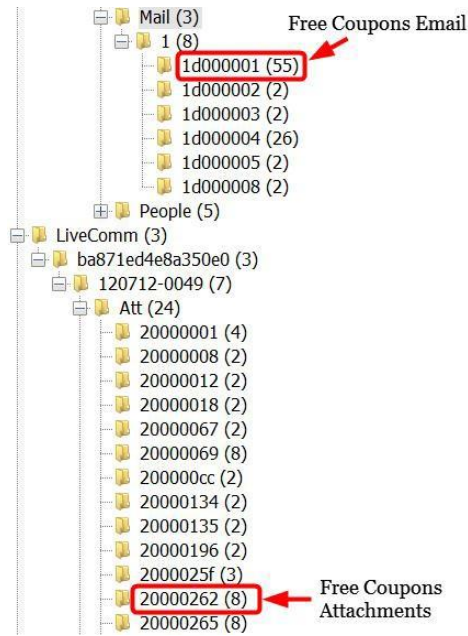
Figure 9-5 - Email Stored under Mail Subfolder and Attachments Stored in Corresponding Att Subfolder

The three jpg files in the Att subfolder match the names of the attachments you saw in the email.
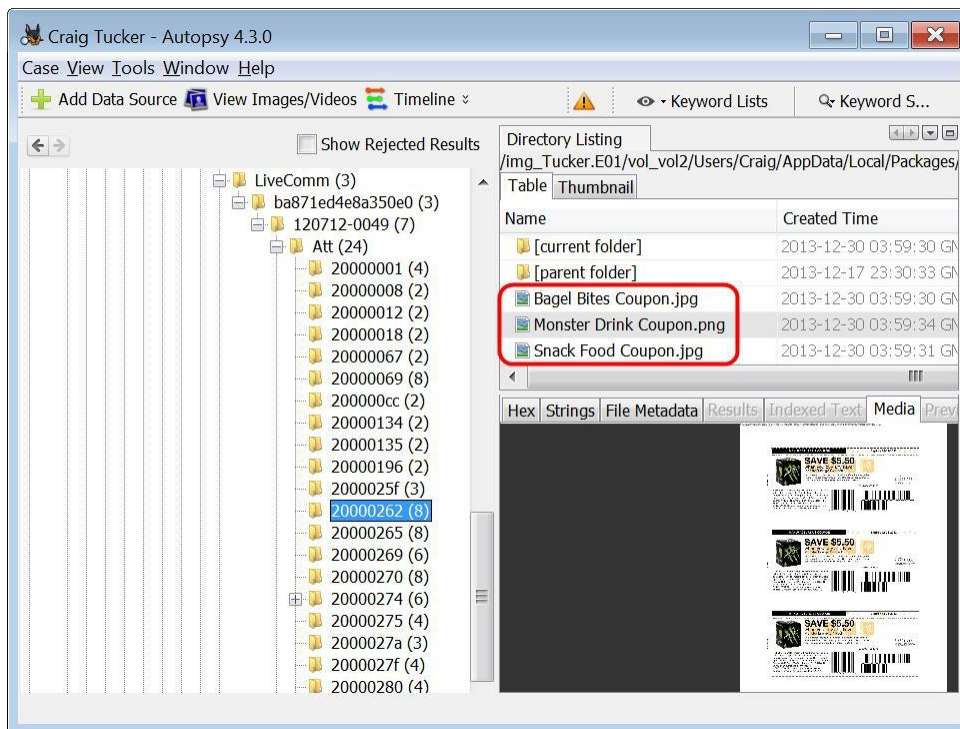
Figure 9-6 - Free Coupons Email Attachments

The Monster Drink coupon was one of the coupons Craig was caught with. Go ahead and tag these three picture attachments.

Windows 10 Mail App

In Autopsy, click on E-Mail Messages under Results in the left pane. As you can see, Autopsy is reporting that there are zero email messages again.
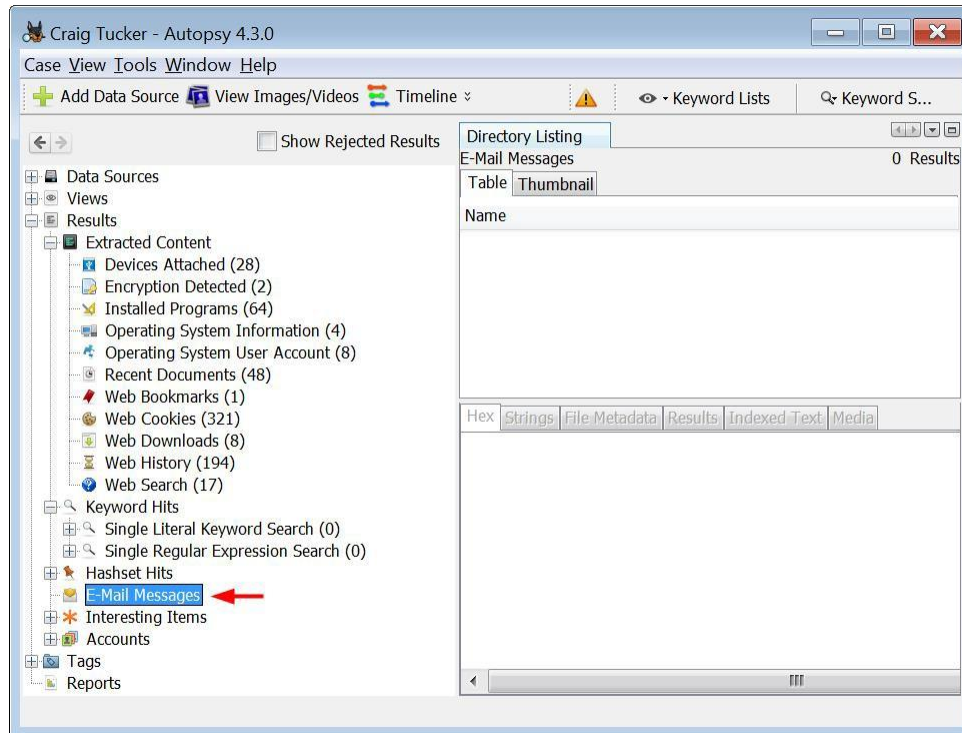
Figure 9-7 – Autopsy Shows Zero E-Mail Messages

Windows 10 Mail stores the emails in the following subfolder:

```
C:\Users\Craig\AppData\Local\Comms\Unistore\data/1/a
```

Once you have navigated to the data folder, there will be numbered folders with corresponding lettered folders containing the emails. The emails are web based in Windows 10 Mail, which means that you cannot simply export them as a .eml file. The files save by default as .dat files now, which for your purposes is a way to save HTML source code and view the email.

The easiest way to convert these to a readable format unless you are comfortable reading html source code is to simply change the file extension to a .html. This will allow you to open the .dat file in a web browser of your choice and see what the formatted message looks like. To do this, open the .dat file in notepad or some other text editor and click the "Save As" button. This will give you the option to change the extension and open it in a web browser. When it is saved, you should have an icon that looks like the web browser that you chose (In this example, Google Chrome was used)
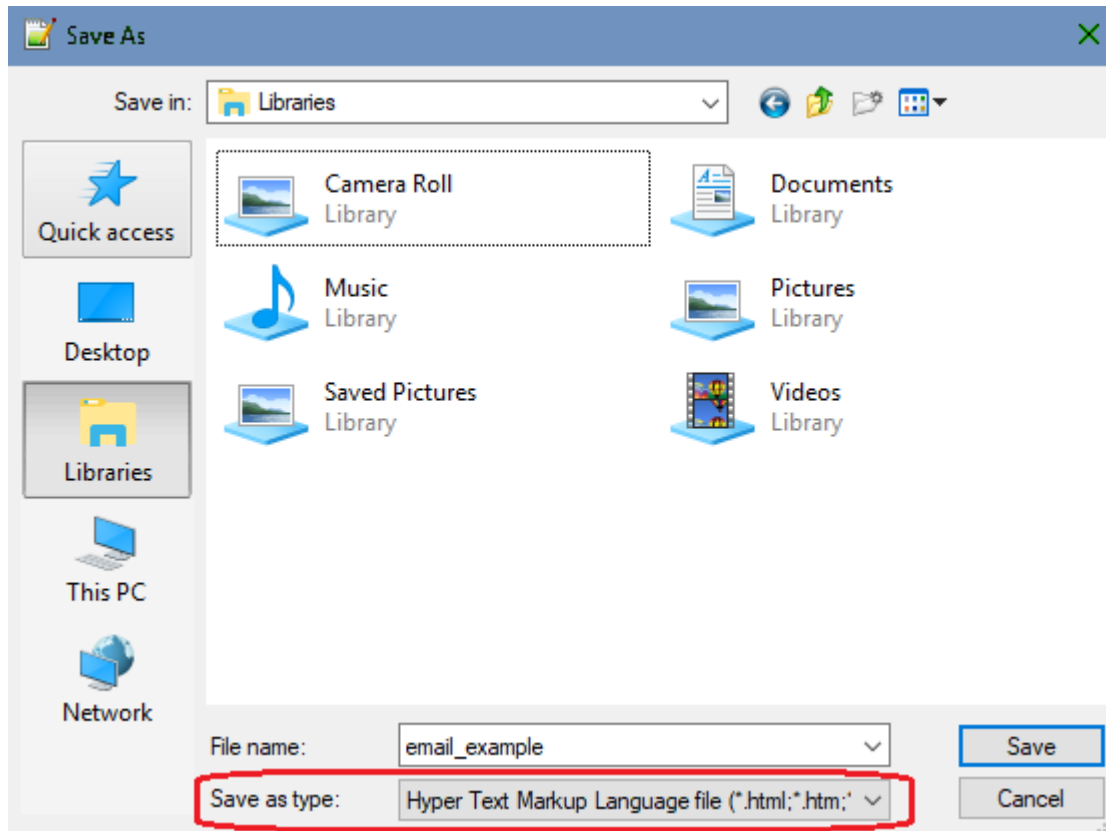
Figure 9-8 – Saving the email as a .html

The new email file will appear wherever you saved it last, so it is recommended to use either the export folder or create an emails folder to place all of the newly converted .html files for easy access. Note that you should include in your report that you had to export and change the extensions, since that is technically modifying evidence and without reason can cause your discovered data to be dismissed.
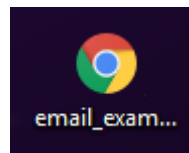
Figure 9-9 – New email_example file that can be opened in a web browser to view

MD5 Hash

There are several coupons in Craig's email attachment folder. If you want to know if Craig has these files saved anywhere else on his computer, you can conduct a search for the coupon based on its MD5 hash value.

A hash value is basically a fingerprint for a file. The chance of two MD5 hash values being the same is 2^{128}. You can use hash values to exclude known files, such as Windows operating system files. There are also "hash libraries", which are large files that contain hash values of alert files, such as CP or hacking software. You can then run these alert hash libraries against the hash values in the image to quickly see if the user has any of these "bad" files.

To find the hash value for files, you will need to run the Hash Lookup plugin. Click Tools►Run Ingest Modules►Tucker.E01. When the Run Ingest Modules window opens, check Hash Lookup and then click Start.
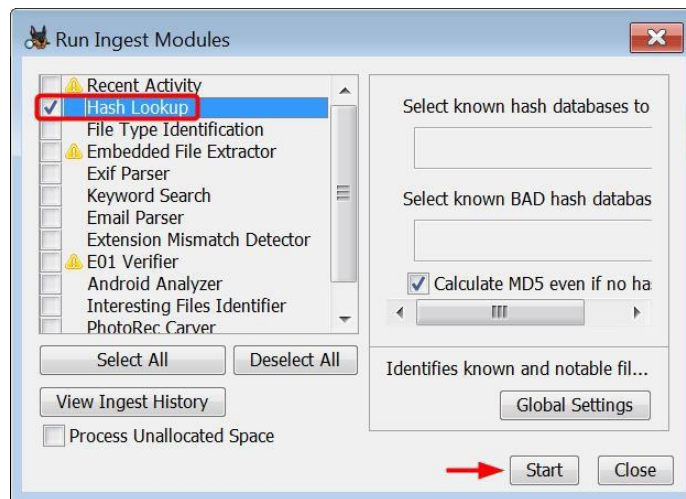
Figure 9-10 – Check Hash Lookup and Click Start

Once Autopsy finishes processing the hash values, take a look at the file 1353033721971.png in the 20000270 attachment subfolder (see Figure 9-8).
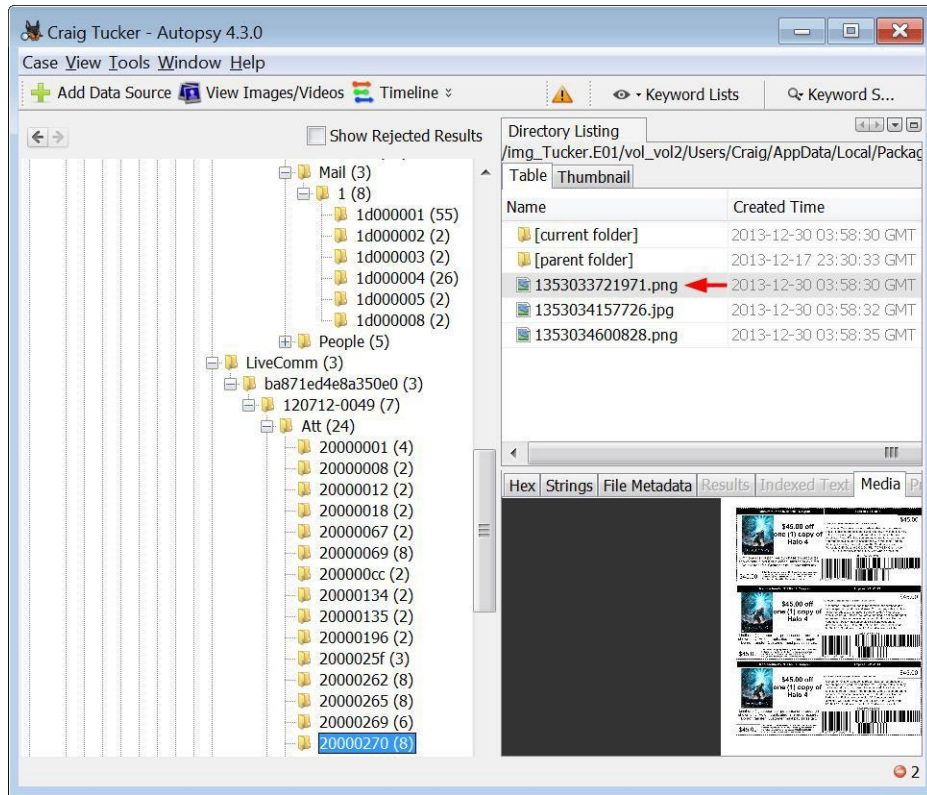
Figure 9-11– Coupon in 20000270 Attachment Subfolder

These attachments come from the 20000270 eml file in the 1d000001 mail subfolder.
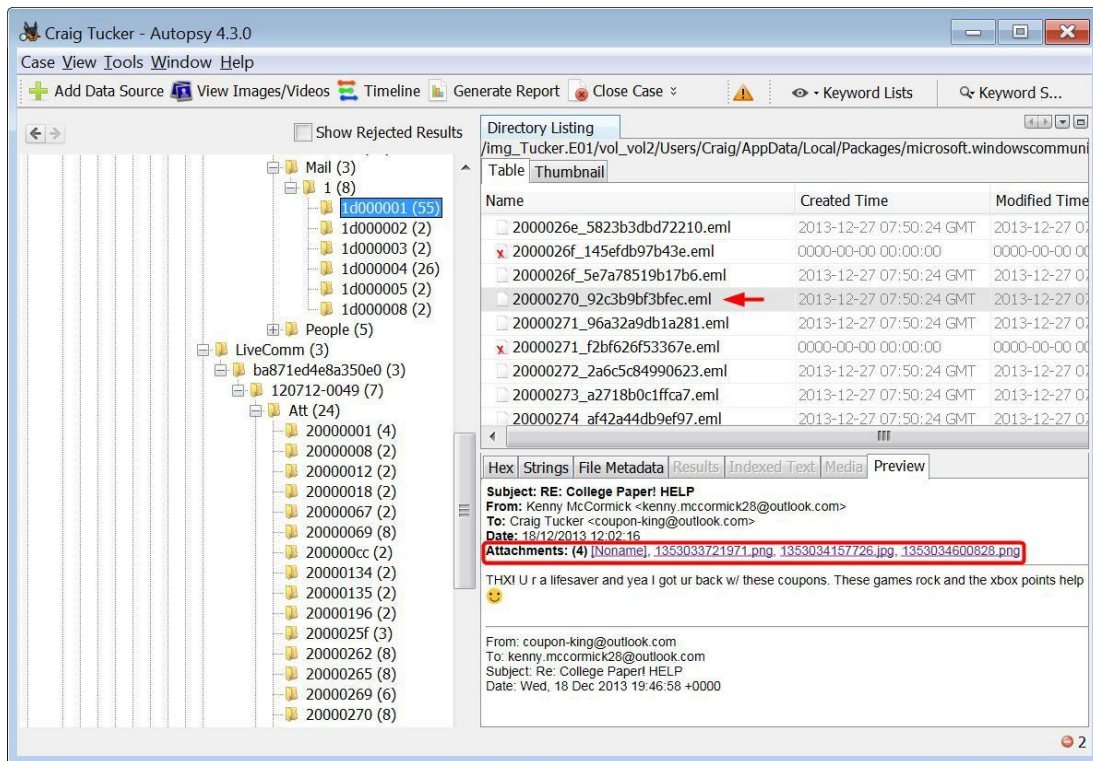
Figure 9-12 – Email with Coupon Attachments

If you want to see if these coupons are saved anywhere else on the computer, right-click the first coupon in the 20000270 attachment subfolder and click Search for Files with the Same MD5 Hash.
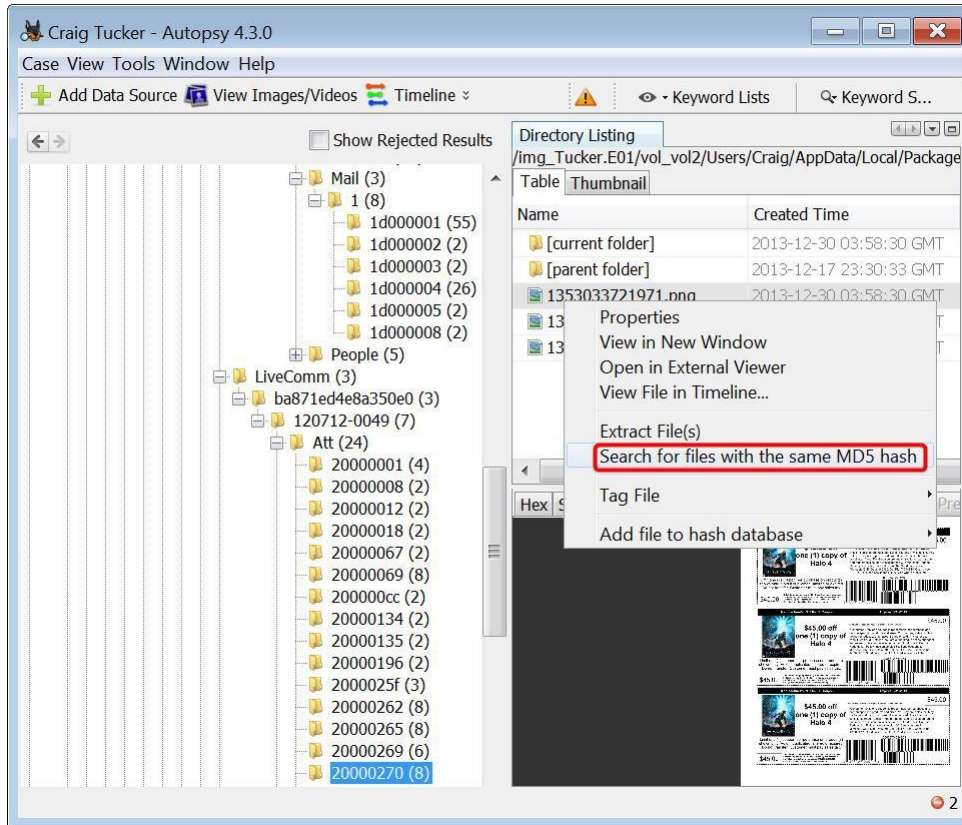
Figure 9-13 – Right-Click Coupon in 20000270 Attachment Subfolder and Search for Hash

There are three matches based on the MD5 hash value. One of the matches is in Craig's My Stuff folder and the other two matches are located in downloaded ZIP files. In the next chapter, you will look into where these downloaded ZIP files came from.

Figure 9-14 - MD5 Hash Match Locations

Email (Continued)

You should continue to look over and tag any emails or attachments of interest to your investigation. One email in particular you should check is the "Re: More Hot Pics", which is under the 20000286 eml in the 1d000004 mail subfolder.

If you remember from earlier, you found link files that pointed to CP. You then found two pictures and a video in the recycle bin. This email mentions "underage pictures", but there aren't any attachments since the original email, "More Hot Pics" is gone. You will go over this later, but tag the email for now.
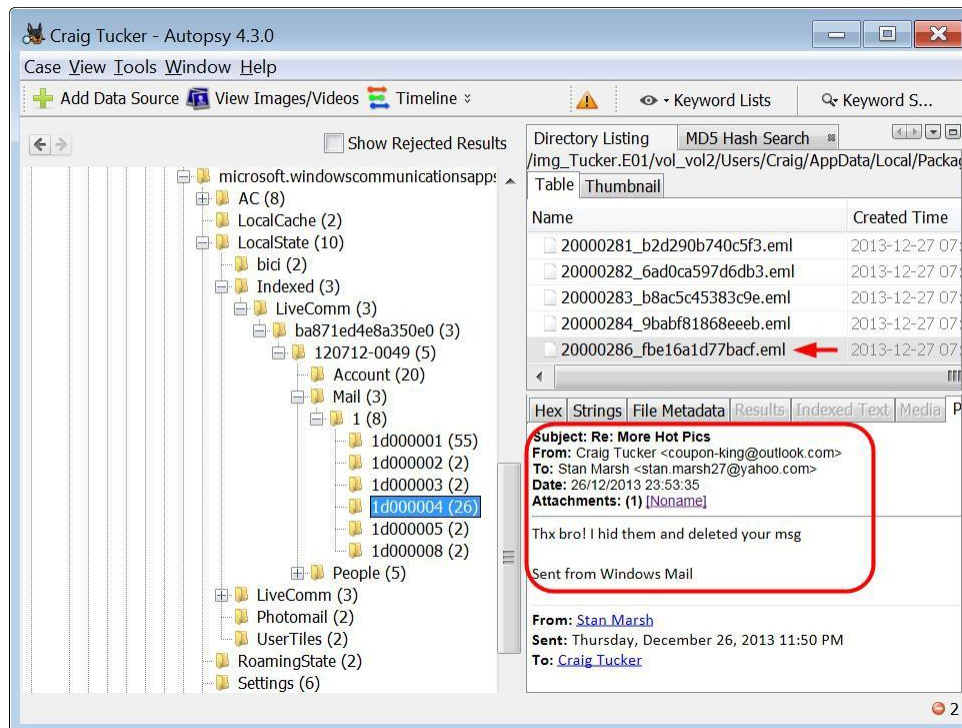
Figure 9-15 – Potential CP Email

Note: The way these emails and attachments are being stored is specific to Windows 8 mail. See Appendix E for information on Windows Live Mail and Mozilla Thunderbird.

Contacts and Keyword Search

With Windows 8 mail, you can see the user's contacts under the People folder, which is located at:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\Indexed\LiveComm\ba871ed4e8a350e0\120712-0049
\People\AddressBook
```

Each file in the AddressBook folder will show a contact name and email address. Craig only has one actual contact: Kenny McCormick.
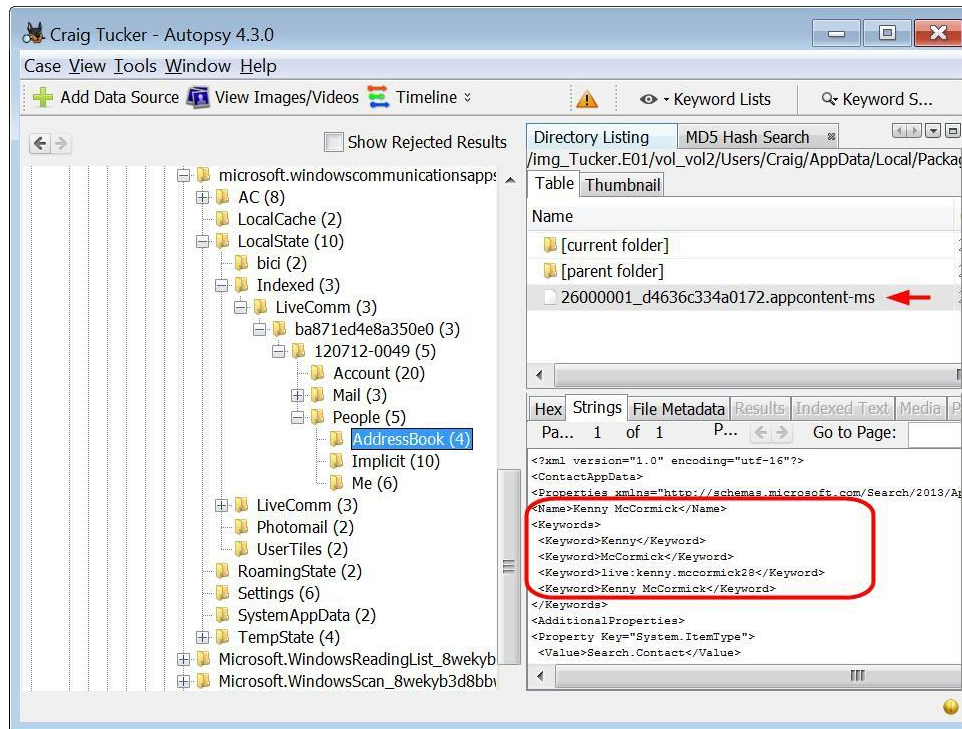
Figure 9-16 - Craig's Email Contact

Look at the subfolder called Implicit under the People folder (see Figure 9-14). Each file in this list shows a name and email address that Craig either sent emails to or received emails from. This information is stored here so when a user begins typing in who the email is "To:", a drop down menu will appear and allow you to auto complete a name or email address.
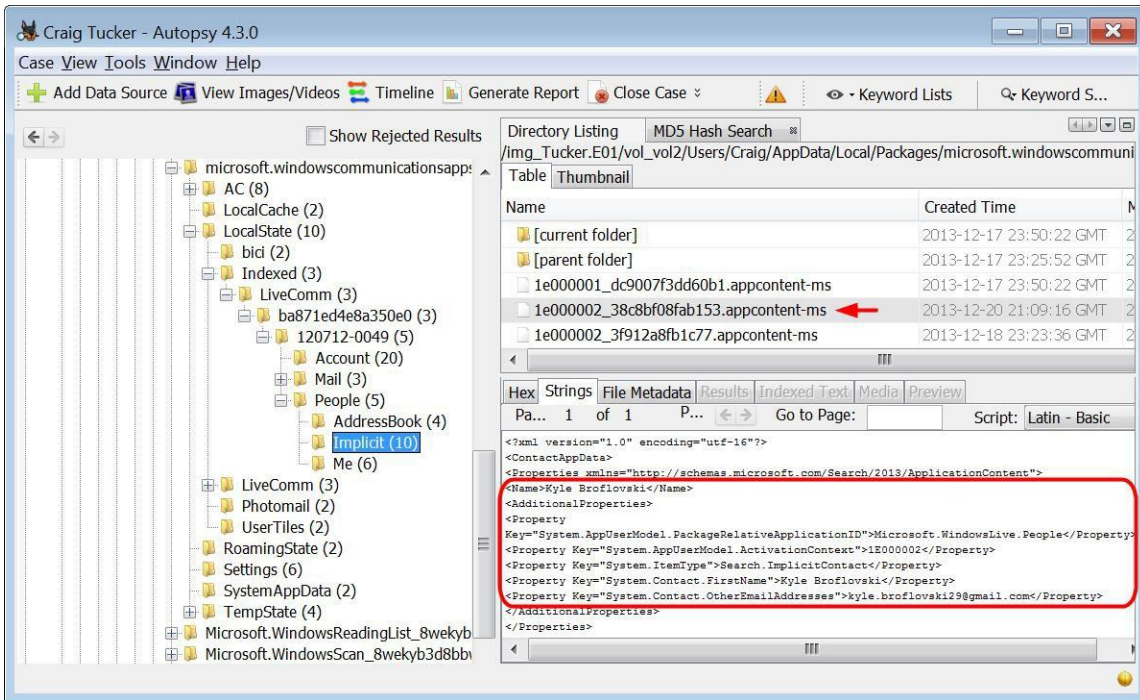
Figure 9-17 - People Craig Sent Email To or Received Email From

Between the AddressBook and Implicit subfolders, you can tell that Craig sent emails to and received email from:

Kyle Broflovski

Stan Marsh

Kenny McCormick

Since Craig was discussing coupons with these three people, go ahead and conduct a Keyword Search for them to see if their names show up anywhere else. To run a Keyword search, you need to first run the Keyword Search plugin. Click Tools►Run Ingest Modules►Tucker.E01. When the Run Ingest Modules window opens, check Keyword Search and click Start.
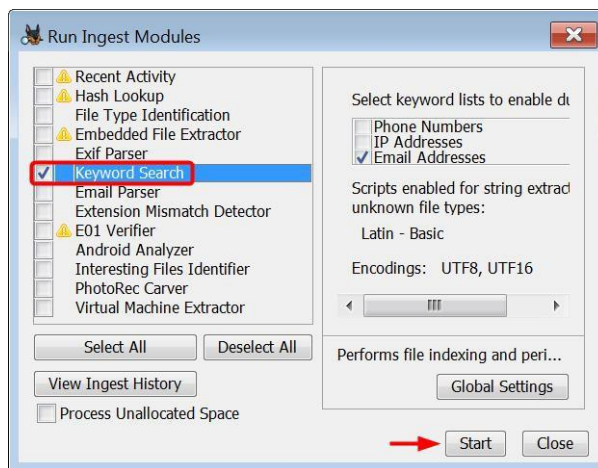
Figure 9-18 – Check Keyword Search Plugin and Click Start

Once Autopsy finishes processing, click the Keyword Search button in the top right corner. Type in Craig's first contact, "Kenny McCormick", and then click the Search button.
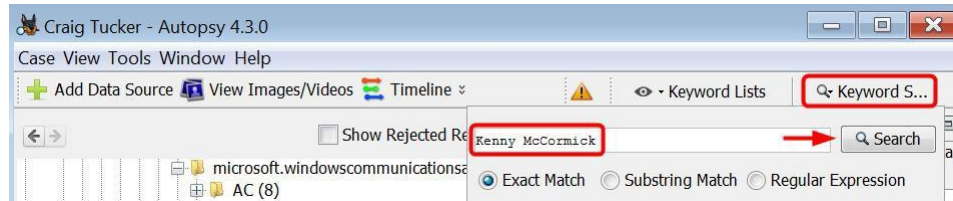
Figure 9-19 – Conduct Keyword Search for Kenny McCormick

You should see several results in the table pane. One keyword search result of particular interest is the main.db file. This file is a database for Skype.

Figure 9-20 – Keyword Search Results for Kenny McCormick

Since there are search hits in the Skype database for Kenny McCormick, this indicates that Craig may have been using Skype to communicate with him. Make note of this, because later you will look into chat programs that Craig may have used.

Computer Forensics CCIC Training

Chapter 10: Internet History

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

10

Internet History

Introduction

Internet history is an important aspect in many cases. You can find out what sites your suspect visited, what they were searching for, and if they downloaded any data. Earlier in the Craig Tucker case, you found files in his Downloads folder. There was a RAR file and two ZIP files that contained several coupons. Where did the suspect download these files from? Some of Craig's email messages also mentioned a "4chan site". What is the 4chan site, and why did Craig visit it? By the end of this section, you will be able to answer these questions and you will have a better understanding of Internet history.

Cookies

Cookies are small pieces of text which is sent to your browser by a website the user visits. The information a cookie stores helps the visited website remember any settings or preferences you specified so that returning to the website will be easier. While companies use cookies to remember your preferences, count visitors, and make relevant ads, investigators can use such information as one way to track the user's browser activity. The following data is stored in the browser's cookies:

Name	The name of the cookie
Content/Value	The value of the cookie **Note:** This is often a string which often represents a session id used by the visited website to recover your session from a larger session state.
Domain	The domain of the cookie
Accessible to script	Yes if Https, No if HttpOnly
Created	The date/time the cookie was created
Expires	The date/time the cookie will expire (typically 1 year from Created) **Note:** If a date/time is not specified then this cookie will remain in the browser until the user deletes it.

When looking at cookies within a browser, the user sees a view similar to this:
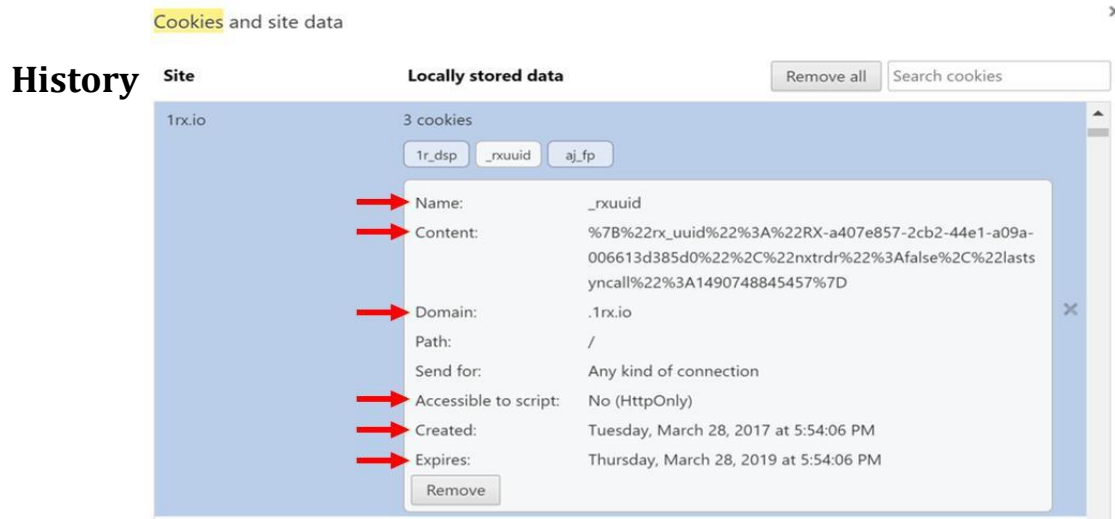
History

Figure 10-1 – Browser View of Cookies

The History SQLite database stores a user's past activity which can be divided into Downloads, History, and Searches.

History	URL	Full URL that was visited by the user
	Date Accessed	Date/time the URL was last visited
	Title	The title of the website visited (ie. Welcome to Facebook)
Downloads	Path	Location of file when downloaded **Note:** This provides you with the downloaded file's name and possible location within the image.
	URL	Full url that was visited by the user to accomplish download
	Date Accessed	Date/time of the download
Searches	Domain	URL where the search was made (ie. google.com, bing.com)
	Text	Text exactly as searched by the user
	Date Accessed	Date/time of the web search

Chrome

Chrome is one of the most commonly used open source web browsers. The browser automatically saves all user activity in all versions of Windows at:

`C:\Users\[`*`username`*`]\AppData\Local\Google\Chrome\User Data\Default`
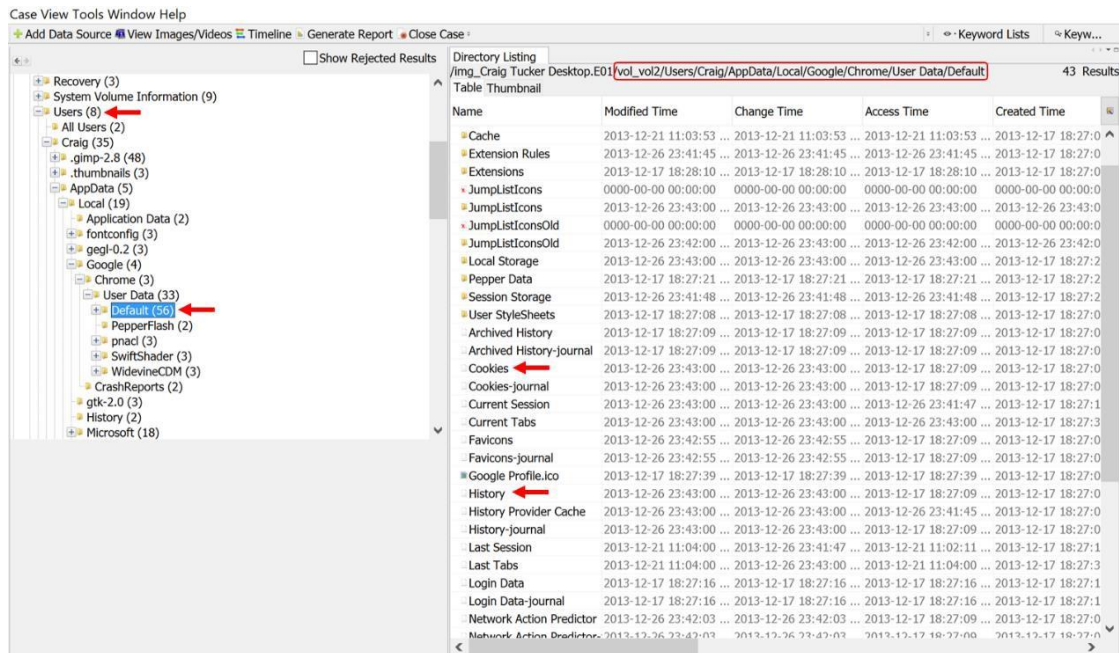
Figure 10-2 – Chrome Cookies and History Database

Internet Explorer

Internet Explorer is another popular web browser and is also the automatic default for Windows computers before Version 10. Being a Windows default, the browser's data is stored within:

```
C:\Users\[username]\AppData\Local\Microsoft\Windows
```
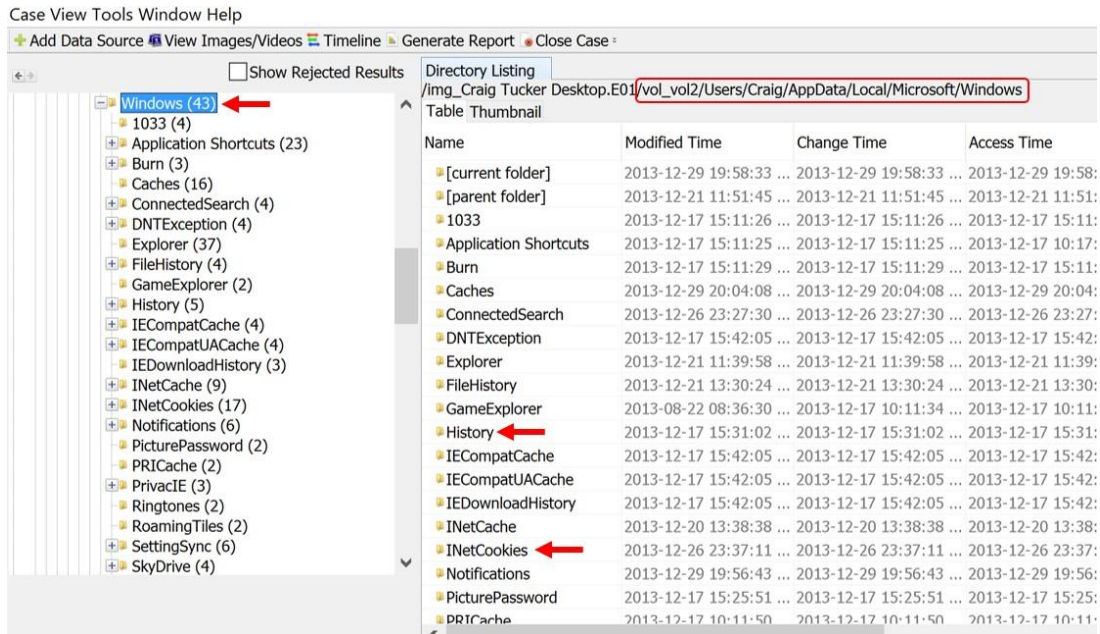

Figure 10-3 – Internet Explorer History and Cookies

SQLite View Example

Next, we will look at the SQLite information you can use to analyze a user's browser activity and how Autopsy makes investigations even easier with the "Extracted Content" window.

In Autopsy, you can view the data stored in SQLite databases by opening the Results view and using the arrows to move between entries. In bold text, at the top of each entry, you will see the word "Web" followed by either "Cookies", "History", "Downloads", or "Search". This tells you of which category the data is considered under (see Figure 10-4).

Note: The same procedure is followed for both Chrome and Internet Explorer browsers. However, this version of Autopsy is not pulling the Internet Explorer history into the Results view. You should always make sure to validate your software and see if it is pulling all the browser history information and determine if the user is using multiple browsers.
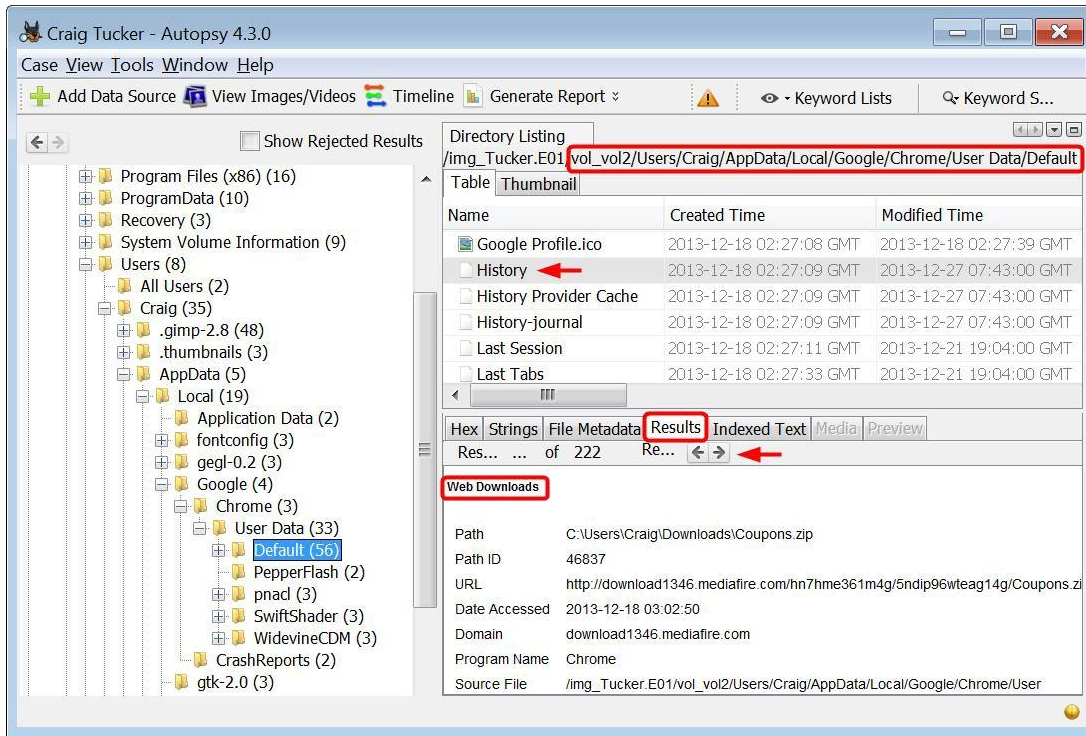
Figure 10-4 – Use Arrows in Results View for Chrome History

The Date/Time shown by Autopsy represents the Created date and time for Cookies as seen below. The Expired data and time are not stored along with whether the Cookie is Accessible to script.
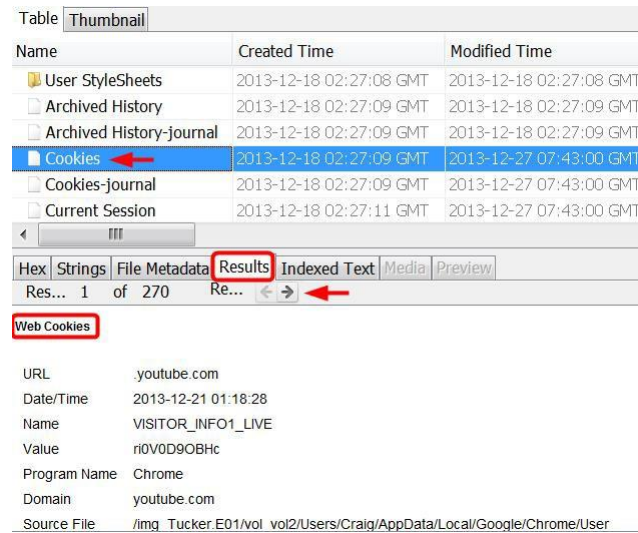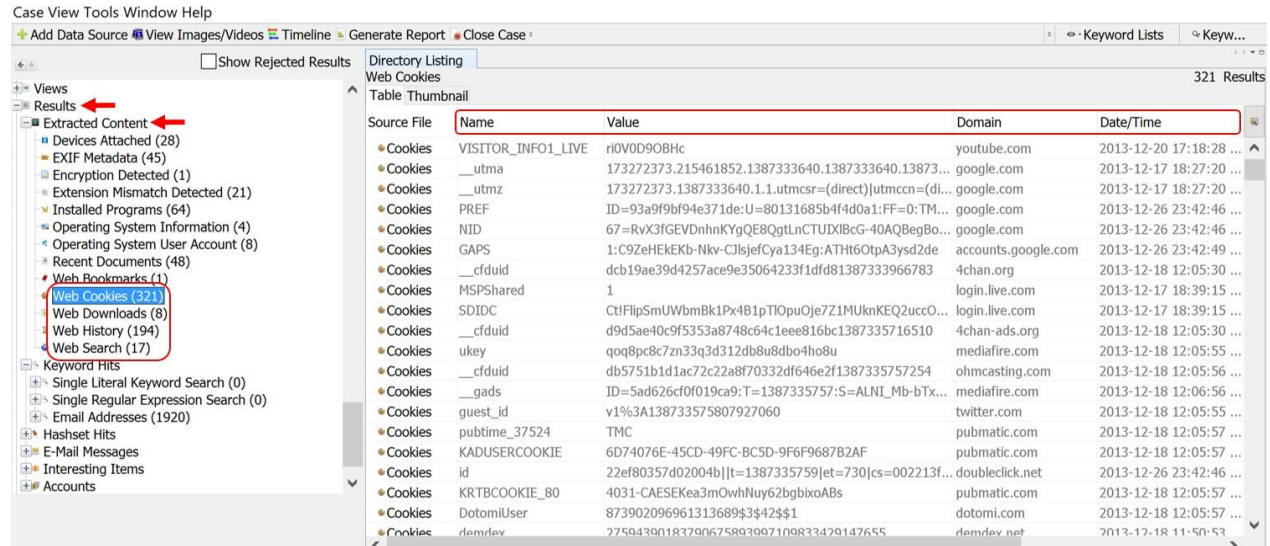
Figure 10-5 – Use Arrows in Results View for Chrome Cookies

Extracted Content View Example

Another way to view the SQLite data in Autopsy is through the Results\Extracted Content window, provided by the program. This window separates each entry into its own "Source File" and then places it within its category of "Web Cookies", "Web Downloads", "Web History", or "Web Search".

Figure 10-6 – Extracted Content View for Web Cookies, Downloads, History, and Search

Note: Under web history, you will see several entries for the website 4chan. People go to this site to post data anonymously to different boards. There are many boards where people will post inappropriate data, but also many fake coupons. People will post their fake coupons to this site so more people will use them and it will be harder to track down who created the coupons and all the people that use the coupons.

CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 11: Chat Logs

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

11

Chat Logs

Introduction

When you ran a keyword search earlier for Kenny McCormick, you found that a search result in the Skype main.db file. The Skype main.db file is used to store chat and contact information for the chat application Skype. It is always important to check chat artifacts because they show who the suspect was communicating with. Many chat programs also support file sharing, so you can see if the suspect shared or received any files through chat.

SkypeLogView

To view Craig's Skype chat logs, you are going to use a tool called SkypeLogView from Nirsoft. It can be downloaded from:

```
http://www.nirsoft.net/utils/skype_log_view.html
```

To use SkypeLogView, you need to export Craig's main.db file (see Figure 11-1). This is located in:

```
C:\Users\Craig\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\
LocalState\live#3acoupon-king_1\main.db
```

Note: This location for the Skype database is specific to Windows 8. In Windows Vista and 7, it was located in:

```
C:\Users\[User Name]\AppData\Roaming\Skype\[Skype Name]
```
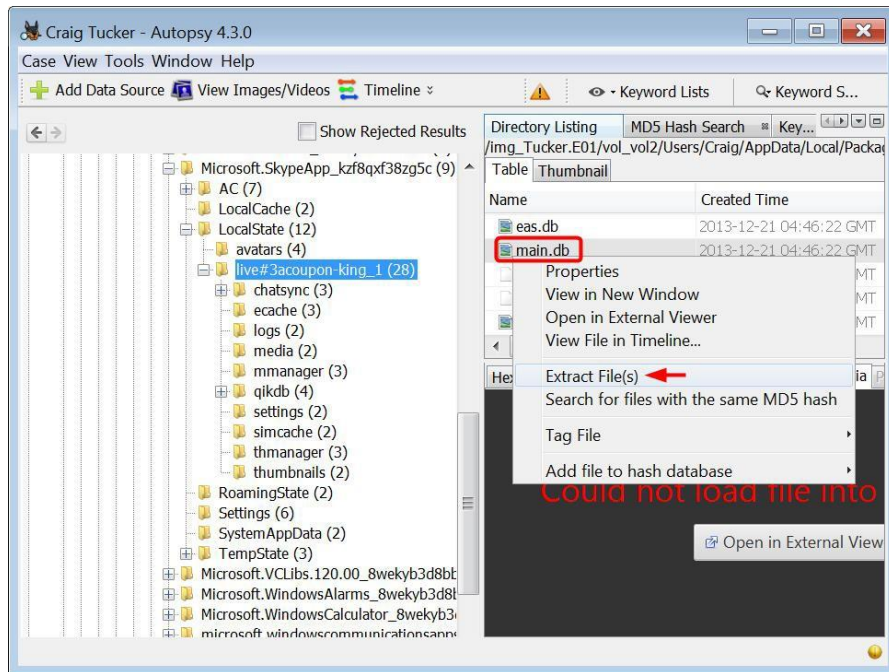
Figure 11-1 – Right-Click Craig's main.db File and Select Extract File(s)

Extract Craig's main.db file to your case Export folder. Open up the SkypeLogView tool. Either type in the location of your case Export folder or use the […] button to browse to your case Export folder. Click OK.
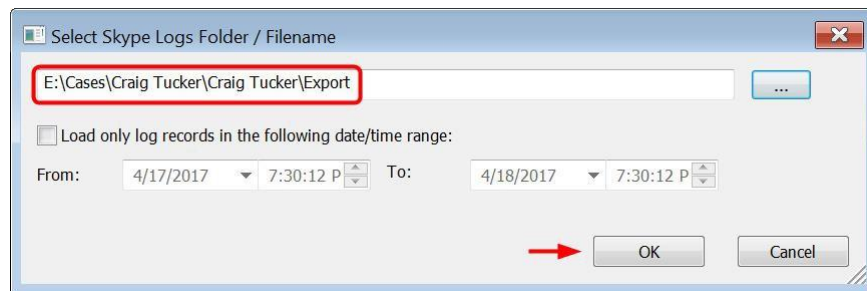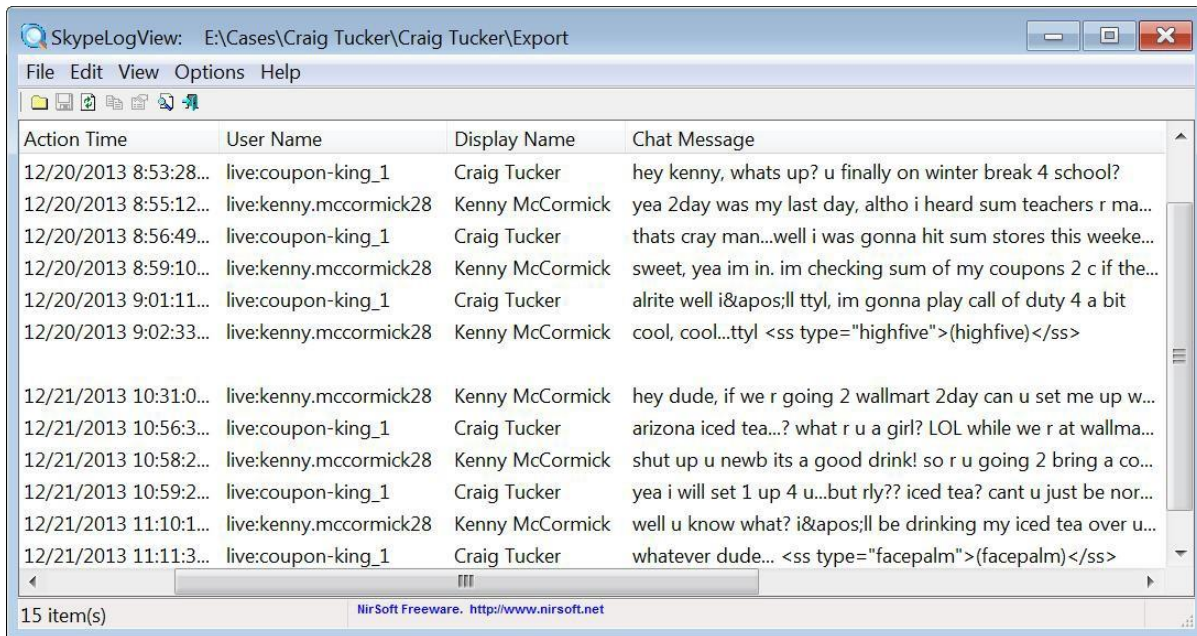

Figure 11-2 – Add Case Export Folder and Click OK

SkypeLogView will parse out all the Skype messages. It will also show who sent the chat message and when it was sent (see Figure 11-3).

Figure 11-3 - Parsed Skype Messages in SkypeLogView

If you click Edit►Select All and then File►Save Selected Items, you can save these messages to an html, csv, or txt report. As you can see through these logs, Kenny had asked Craig to get him the Arizona Iced Tea coupon.

Computer Forensics CCIC Training

Chapter 12: Hidden Data

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

12

Hidden Data

Introduction

There are several ways suspects will try to hide their data. A very common way suspects will usually hide their data is through encryption and passwords. However, they might also try to change file extensions or create hidden files and folders. Not every suspect will try to hide their data through these methods, but it is still important for you to be aware of the different data hiding methods. Once you know how some suspects might try to hide their data, you can learn how to better detect and handle passwords or renamed file extensions.

Passwords and Encryption

Towards the beginning of your analysis, you came across a password protected word document and ZIP file on Craig's desktop. Both file names had the word coupon in it, which means that these files could contain data relevant to your case. You are going to attempt to decrypt these files.

A good method to use when attempting to break a file's password is to follow a phased approach (see Figure 12-1). With a phased approach, you first try the easiest method, which is usually trying any known passwords, such as the user's login password. You can also try to run an English dictionary attack. If those both fail, you can index the suspect's drive and create a word list from the indexed words. The word list can then be used as a dictionary attack. Many criminals are lazy and will save passwords in places on their computer, reuse passwords for multiple accounts, and have physical versions like sticky notes and papers with passwords written on them. Be sure to check all of these sources when doing a real investigation before resorting to the brute force method. If the password is still not broken after all of these attempts, you can try a brute force attack.

The brute force attack method is usually a last resort. It goes through every possible combination of uppercase letters, lowercase letters, numbers, and symbols. A brute force attack will work eventually, but it takes a great deal of time and resources.
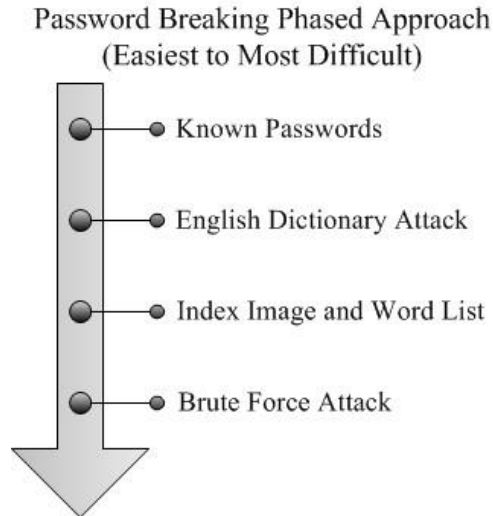
Figure 12-1 - Phased Approach to Breaking Passwords

First, you are going to try to use Craig's login password on the MyCoupons.zip and AWESOME COUPONS.docx. Export both these files out of Autopsy and save them into your Export folder.
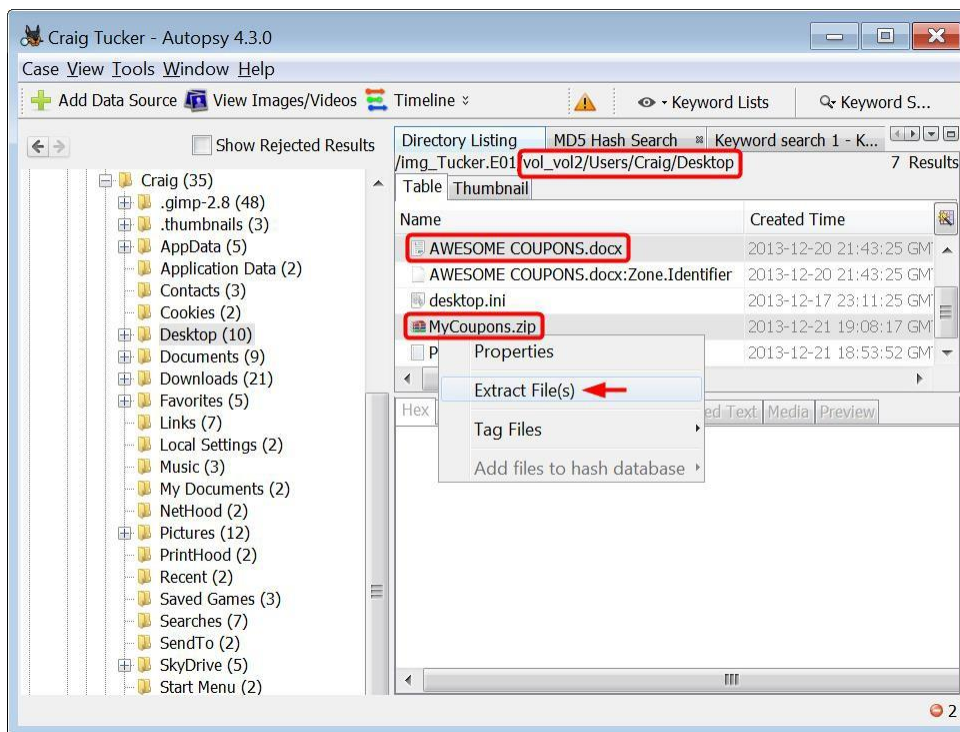
Figure 12-2 – Extract MyCoupons.zip and AWESOME COUPONS.docx in Craig's Desktop Folder

Once MyCoupons.zip is in your case Export folder, you are going to need a tool to open it with, such as 7-Zip or WinRAR. You can download 7-Zip at:

```
http://www.7-zip.org/download.html
```

Once you have the 7-Zip tool, right-click MyCoupons.zip and click 7-Zip►Open Archive (see Figure 12-3).
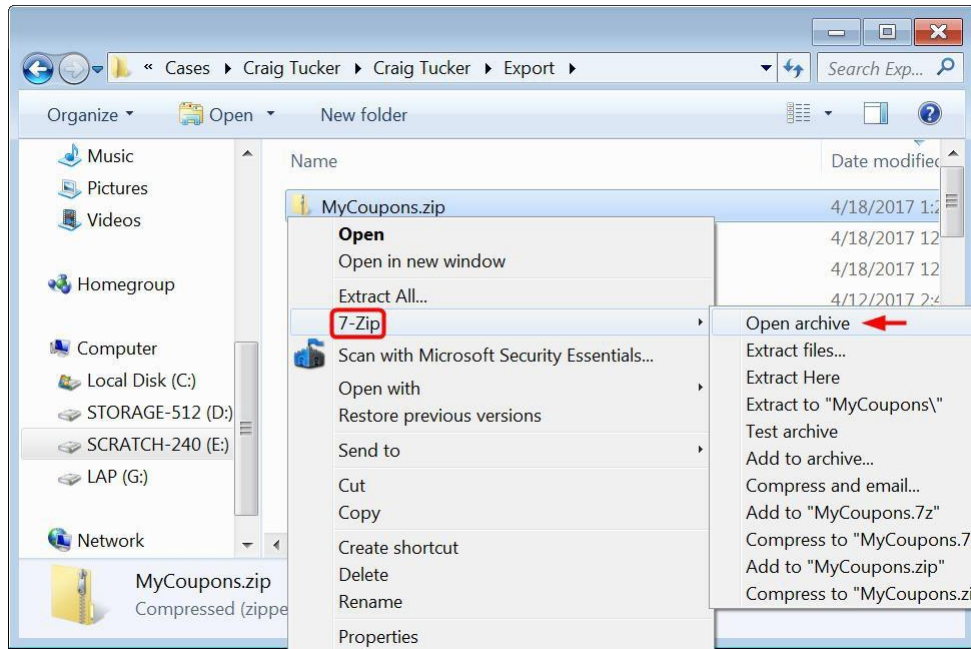
Figure 12-3 – Right-Click MyCoupons.zip and Select Open Archive under 7-Zip

When 7-Zip opens, highlight all the files and click the Extract button in the top bar.
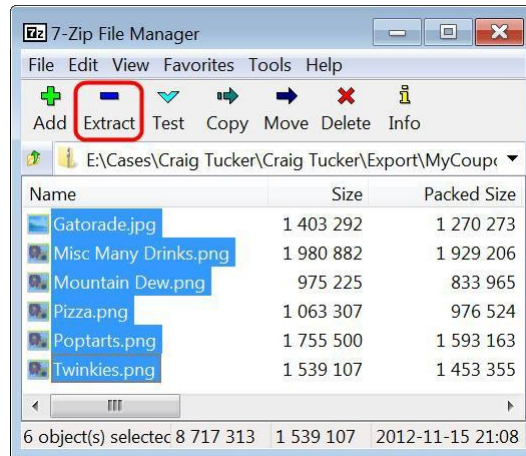
Figure 12-4 – Highlight All Files and Click Extract Button

7-Zip will prompt you with a Copy window. Create a subfolder under your case Export folder and then click OK (see Figure 12-5).
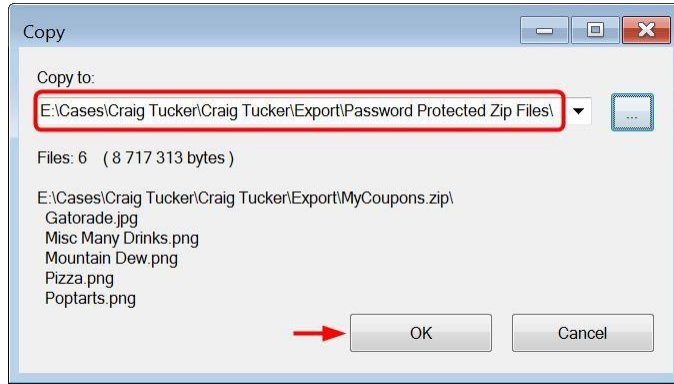
Figure 12-5 – Create Subfolder under Case Export Folder and Click OK

Next, you need to type in Craig's login password "hungry123" and then click OK.

Figure 12-6 – Type in Craig's Login Password and Click OK

Now you can view the decrypted password protected zip files.
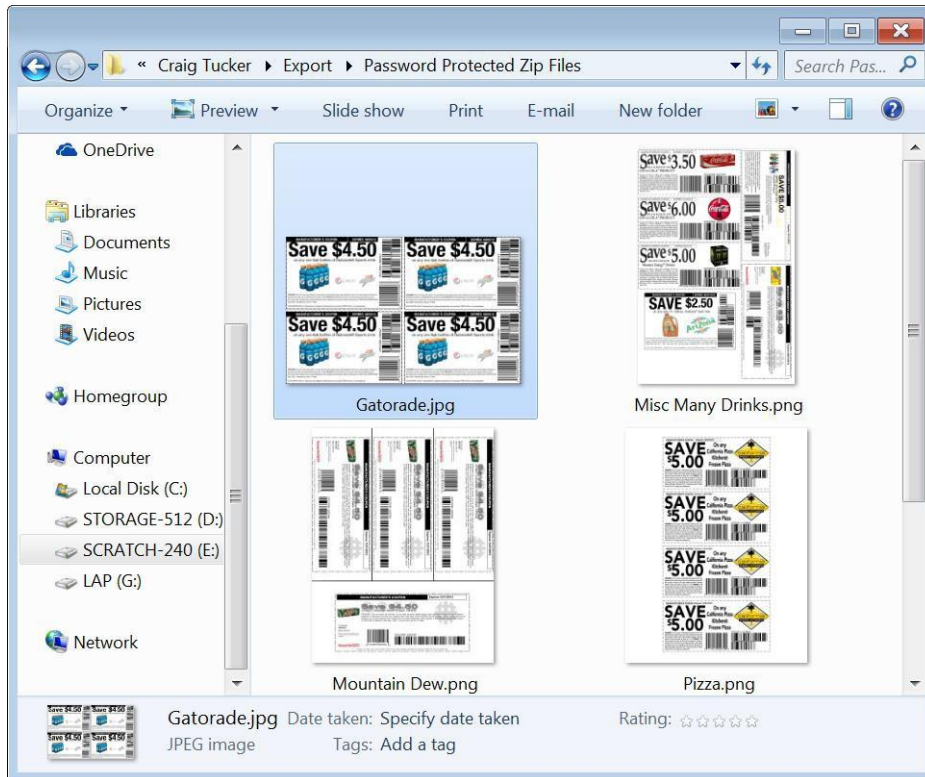
Figure 12-7 – Password Protected Zip Files Decrypted

Now you should try to open Craig's AWESOME COUPONS.docx file with the same login password. When you open the file, you should be prompted with a Password window. Type in hungry123 and click OK.
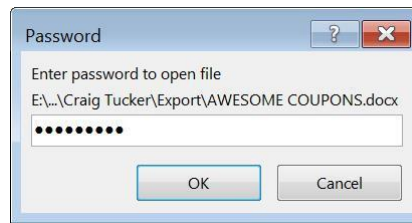
Figure 12-8 – Type hungry123 for AWESOME COUPONS.docx

The program should tell you that the password is incorrect. If you were to try and find the password for this Word document, you would then want to look if the suspect wrote any passwords down or had sent any in emails or chat. You could also then follow the phased approach and next try an English Dictionary Attack with password breaking software.

Signature Analysis

Sometimes users have suspicious data they do not want deleted, but rather hidden. Users can accomplish storing data yet hiding its true nature by simply changing the file's name and/or extension. For example, a user could change naughty_photo.jpg to water_bill.txt in order to revert attention to the file. The change in file extension, however, is detectable through signature analysis. Each file has a signature embedded in itself which can then be compared to what the file claims to be. When these two pieces of information do not match, the investigators know a more detailed analysis of the file is required. The following are the "magic numbers" for common file types:

File Type	Extension	Magic Number / Hex Value
JPEG Graphic	.jpg	FF D8
PNG Graphic	.png	89 50 4E 47 0D 0A 1A 0A
MP3 Audio	.mp3	49 44 33
AVI Video	.avi	52 49 46 46
MOV Video	.mov	6D 6F 6F 76
Windows Video File	.wmv	30 26 B2 75 8E 66 CF
PDF	.pdf	25 50 44 46
Rich Text Document	.rtf	7B 5C 72 74 66 31
Word / Excel / PowerPoint Document	.doc / .xls / .ppt	D0 CF 11 E0 A1 B1 1A E1

These specific hex values (also known as "magic numbers") are at the beginning of each file and identify the file's type based on its content, not its file extension.

For additional signatures, you can use a File Extension Seeker or File Signature Table such as:

```
http://file-extension.net/seeker/
https://en.wikipedia.org/wiki/List_of_file_signatures
```

Windows uses a file's extension to determine what program to use to open or execute a file. For example, if there is a picture called Stuff.jpg, it will be opened with Windows Photo Viewer or another picture viewing program by default. However, if the file is renamed to Stuff.txt, it will be opened with Notepad or Word by default and it will look like Figure 12-9.

Figure 12-9 - Picture Renamed to Text File, Windows Opens Picture in Notepad by Default

Extension Mismatch Detector

One way to view the files that are suspicious and possible candidates of a user-modified file extension is to use Autopsy's Extension Mismatch Detector plugin. Click on Tools►Run Ingest Modules►Tucker.E01. When the Run Ingest Modules window opens, check Extension Mismatch Detector and then click Start.
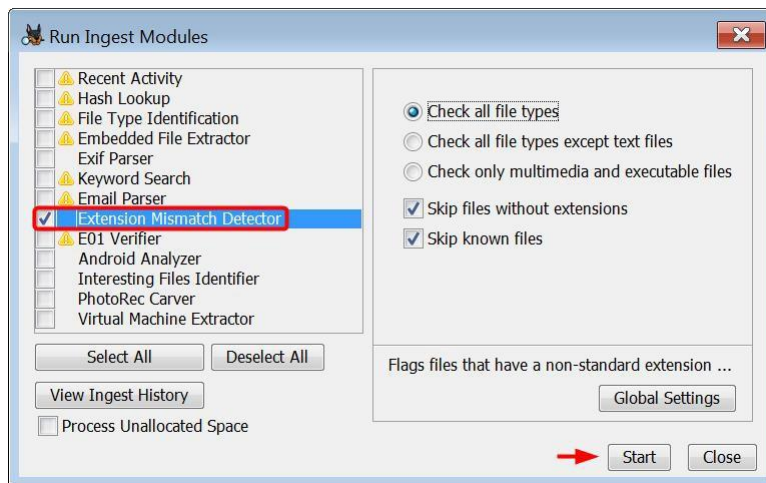

Figure 12-10 – Check Extension Mismatch Detector and Click Start

When Autopsy finishes running, you can view the results in Results\Extracted Content\Extension Mismatch Detected window. This window is where Autopsy places any files that it finds during analysis whose signature possibly does not match its defined extension (see Figure 12-11).
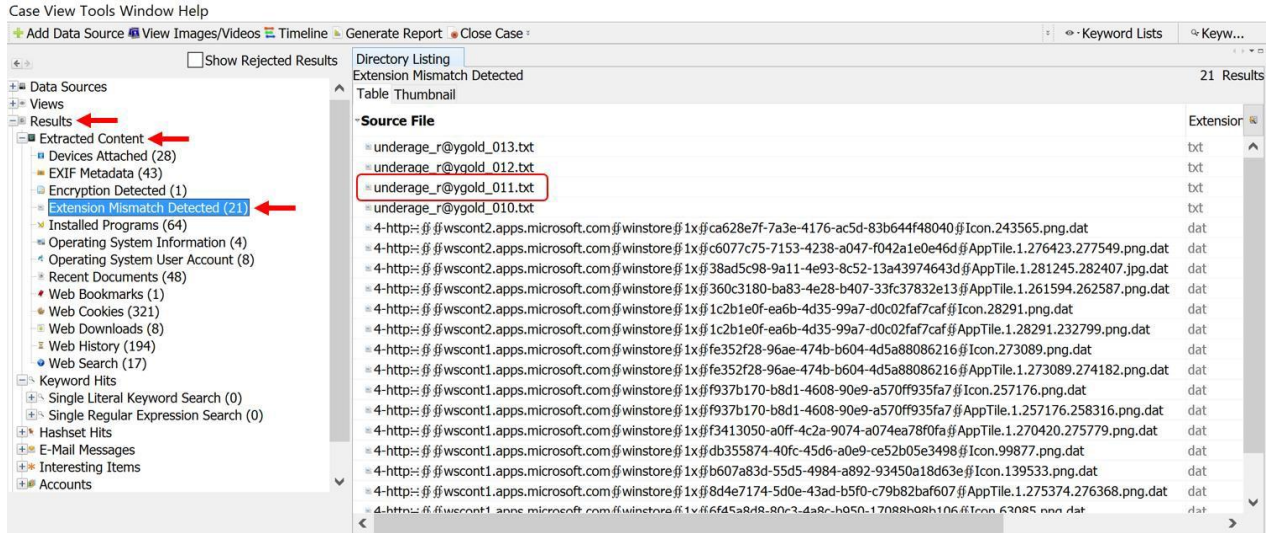
Figure 12-11 – Results for Extension Mismatch Detector Plugin

Click the Extension column in the Table pane, and scroll down to the entries with txt. As you can see there are four text files of interest all with the names underage_r@ygold. Autopsy has determined based on the hex header of these files that they are actually jpeg images and not text files.
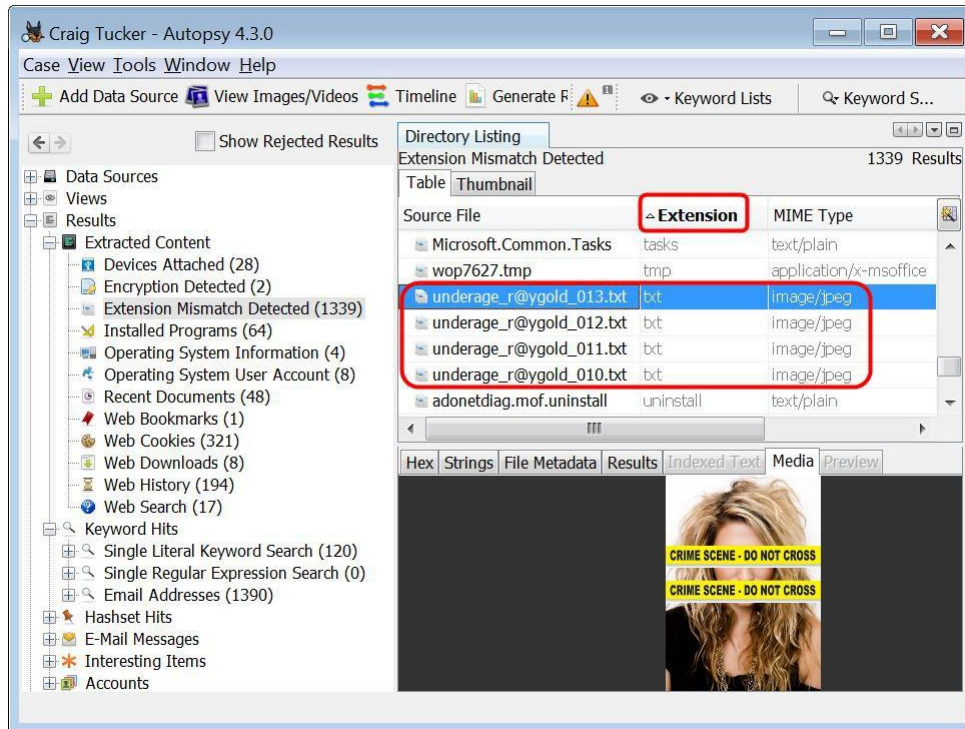
Figure 12-12 – Sort by Extension Column and View Text Files that are Images

Note: The problem with this category is that it comes back with many results that are not useful. It's true that these files' extensions don't match their headers, but that does not mean the suspect intentionally renamed the extensions. There are several Windows system files and programs files that have mismatched headers and extensions.

Hex View Example

In Autopsy, navigate to the location of the file that you deem as suspicious and open it in Hex view. Open the file "underage_r@ygold_011.txt" to check its contents, as it seems suspicious.

Figure 12-13 – Right-Click One of the Text Files and Click View Source File in Directory

Autopsy will take you to the folder where these pictures are being stored, which is the following path (see Figure 12-14):

```
C:\Windows\System32\system files
```

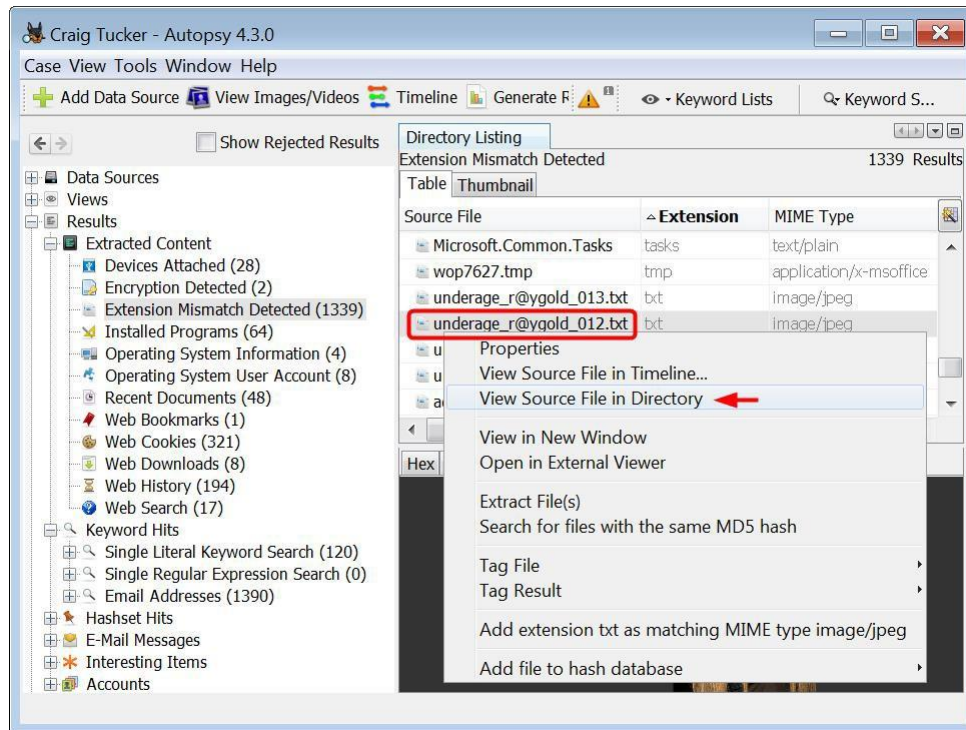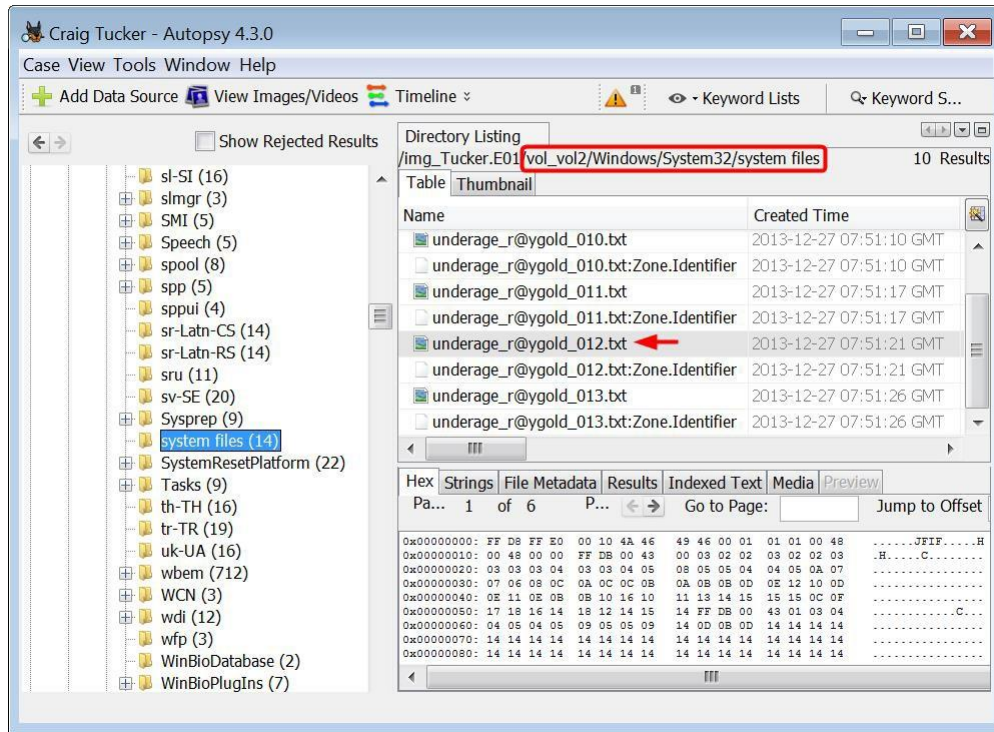**Figure 12-14 – Renamed Picture Files Stored in system files Subfolder**

View one of these picture files in hex view and look at the header. As you can see it has a header of a JPEG Graphic file.
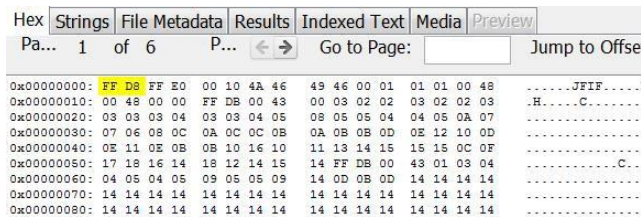
Figure 12-15 – JPEG Graphic File Header on Renamed Text File

When you compare the extension of "underage_r@ygold_011" with the file type found from the signature, you should have a mismatch. The signature matches a JPEG Graphic file with "FF D8", rather than that of a Plain Text File (.txt). Therefore, you as an investigator should do more analysis on the file since the user was attempting to keep its contents hidden.

CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 13: Installed Programs

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

13

Installed Programs

Introduction

Looking at what programs your suspect had installed can start to give you a better idea of how they used their computer. If he had pictures, how did he view or edit them? If he had ZIP and RAR files, how did he open them and extract data? If he had digital movies, how did he play them?

In this section, you will be looking at three specific programs. Programs are almost never the same, so information about how they were used will be stored differently. You can often find information about a program from its website. You can also try downloading the program on a virtual machine with the same OS as your suspect to see what it does and how it is storing evidence on your suspect's computer.

Take a look at what programs are installed on Craig's computer. You can find installed programs under:

```
C:\Program Files
C:\Program Files (x86)
```

The first program you are going to look at is GIMP 2.
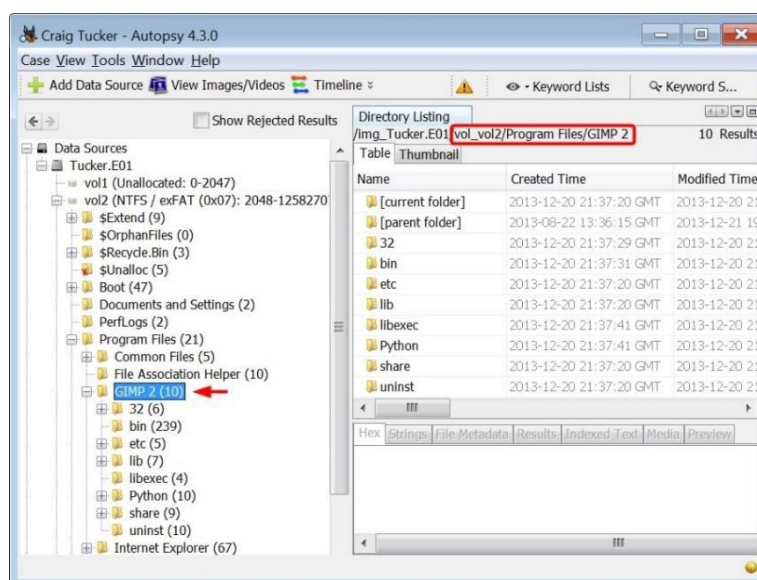
Figure 13-1 – GIMP 2 in Program Files

GIMP

GIMP is a freeware graphic manipulation tool. You can alter pictures and add layers to a photo with it. If you look at Craig's email, there is one called "Re: Coupon Making" from Stan Marsh. Craig had asked him how to make his own coupons, and then Stan attached two guides and told him to download GIMP.

Figure 13-2 – Email Mentioning GIMP

Go to Craig's downloads folder in:

```
C:\Users\Craig\Downloads
```


Figure 13-3 – GIMP Installer in Downloads Folder

As you can see, Craig downloaded the installer for GIMP and then installed it.

Something that is unique to GIMP is that it has a "document history." This document history feature is so users can easily find and open their recently used files.
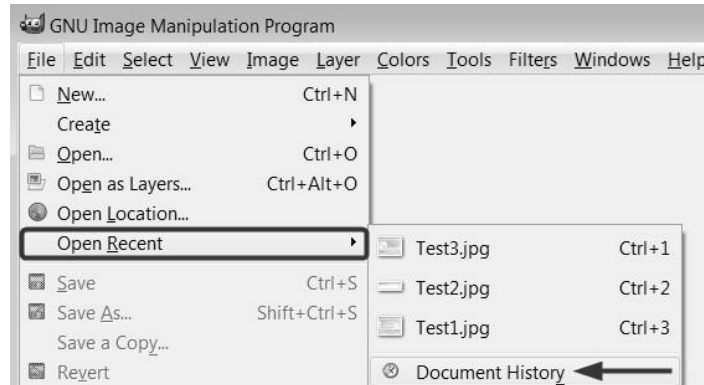
Figure 13-4 – GIMP Document History

The document history is being stored in:

```
C:\Users\Craig\AppData\Local
```

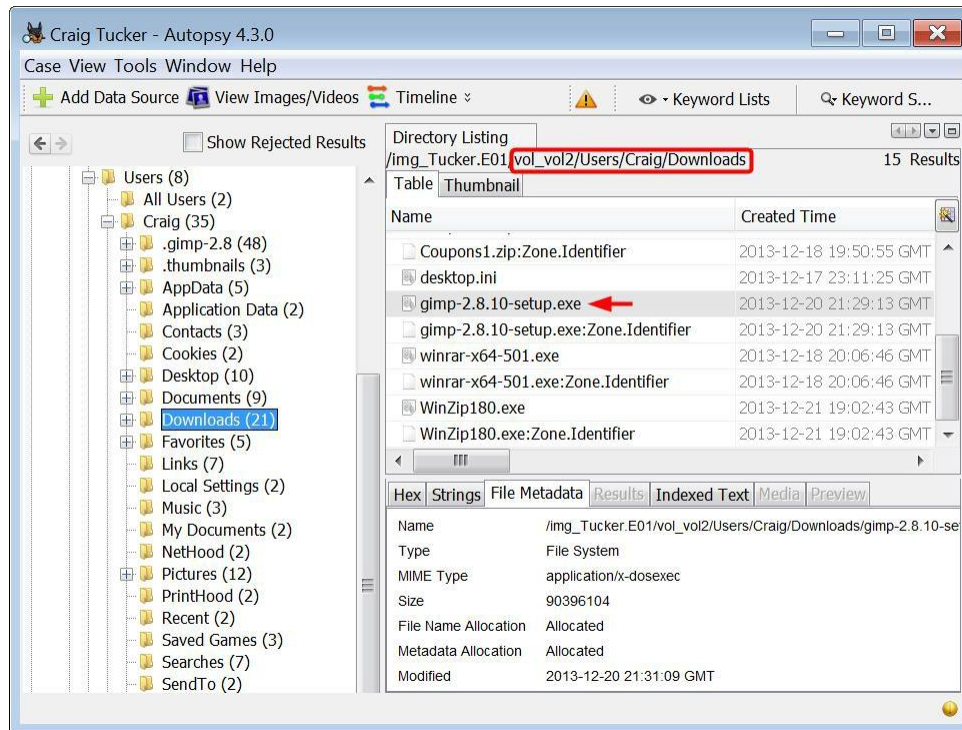In the Local folder, there is a file called recently-used.xbel. This is an XML-formatted file that contains information about the pictures that Craig had opened with GIMP.
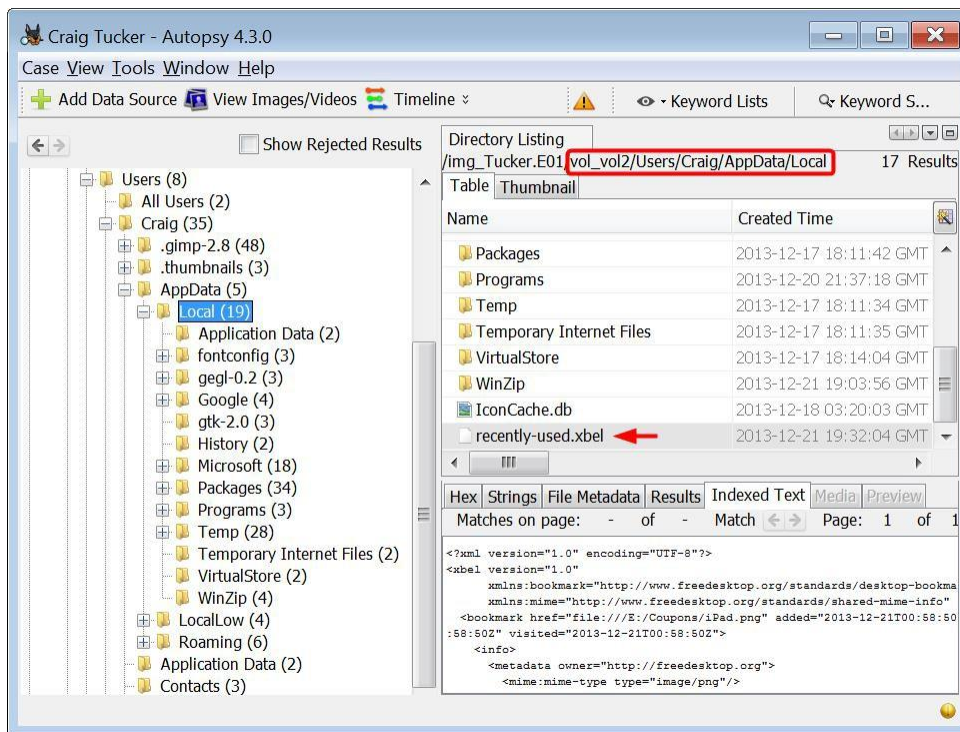
Figure 13-5 - GIMP Document History Stored in XML File

If you look in the XML file in Indexed Text or Strings view, there are several entries that appear to be coupons. He opened these on his drive and from his external drive. The XML file even gives you the date and time when each file was opened (see Figure 13-6).

Figure 13-6 - Entries in GIMP Document History

You don't have Craig's E: drive, so you can't look at most of the picture files that he opened with GIMP. However, you can look for "1304644031008.png" and "Iced tea – edited.png" in his My Stuff folder.

Double-click the Created time column to sort the files by created time. If you look at the bottom of the list, you will see a file called "1304644031008.png" and "Iced tea - edited.png".

Look at the first Arizona Iced Tea coupon named 1304644031008.png. It has a file Created time of 12/21/2013 at 19:14:07 GMT.
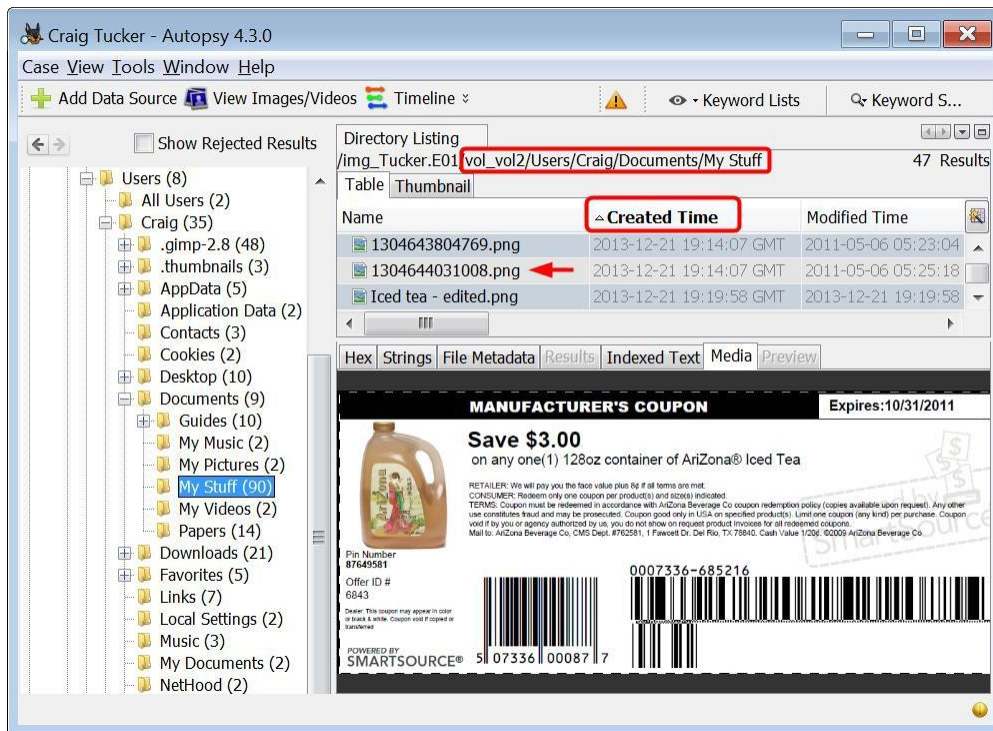
Figure 13-7 - Iced Tea Coupons in Craig's My Stuff Folder, Sorted by Created Time

To know if these files were created on Craig's computer at that time or if they were copied from another source, you can look at the Created time for the other files. Nine of the other coupons have a Created time of 12/21/2013 at 19:14:07 GMT.

Now, look at the Modified times of these 10 files. These times predate the Created time. Based on these time stamps, this activity is consistent with these files being copied to the My Stuff folder from another source, such as his external E: drive.

Table	Thumbnail	
Name	△ Created Time	Modified Time
1304377546277.jpg	2013-12-21 19:14:06 GMT	2011-05-03 05:59:12 GMT
1304377950804.png	2013-12-21 19:14:06 GMT	2011-05-03 05:59:52 GMT
1304393958244.png	2013-12-21 19:14:06 GMT	2011-05-03 08:24:16 GMT
1304394230314.jpg	2013-12-21 19:14:06 GMT	2011-05-03 08:23:44 GMT
1304644210039.png	2013-12-21 19:14:06 GMT	2011-05-06 05:25:22 GMT
1304400692832.png	2013-12-21 19:14:07 GMT	2011-05-03 08:36:40 GMT
1304643149337.png	2013-12-21 19:14:07 GMT	2011-05-06 05:20:18 GMT
1304643663005.png	2013-12-21 19:14:07 GMT	2011-05-06 05:22:20 GMT
1304643804769.png	2013-12-21 19:14:07 GMT	2011-05-06 05:23:04 GMT
1304644031008.png	2013-12-21 19:14:07 GMT	2011-05-06 05:25:18 GMT
Iced tea - edited.png	2013-12-21 19:19:58 GMT	2013-12-21 19:19:58 GMT

Figure 13-8 – Timeline of Coupons

The edited version of the Arizona Iced Tea coupon (Iced tea – edited.png) was created approximately 5 minutes later on 12/21/2013 at 19:19:58 GMT. The Modified time of Iced tea- edited.png matches the Created time, which is consistent with this file being created on this computer.

WinZIP

The next program you are going to look at is called WinZIP. WinZIP allows you to zip and unzip files. You can also use it to create password protected ZIP files. Earlier, you found that Craig downloaded ZIP files that contained several coupons.

WinZIP keeps some information stored in the user's NTUSER.DAT file. Open up Craig's NTUSER.DAT file with Registry Explorer, and navigate to:

```
Software\Nico Mak Computing\WinZip
```
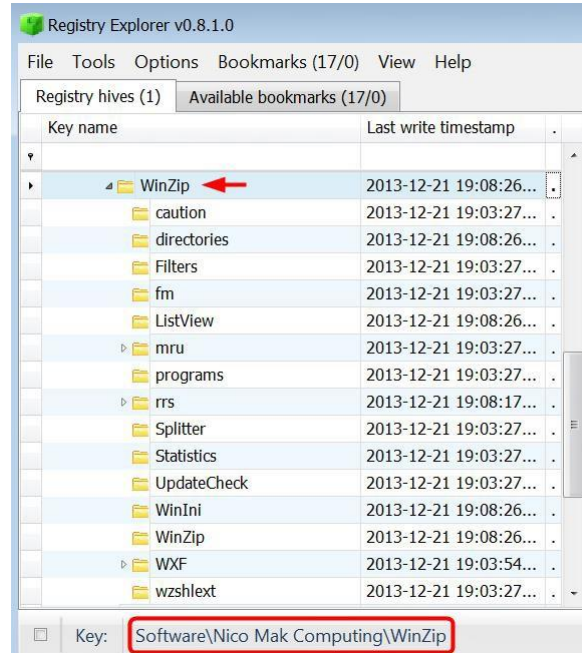

Figure 13-9 - WinZip Key in Craig's NTUSER.DAT

Under the WinZip subkey, there are several other subkeys. The "directories" subkey contains value names of "AddDir" and "ZipTemp" (see Figure 13-10).
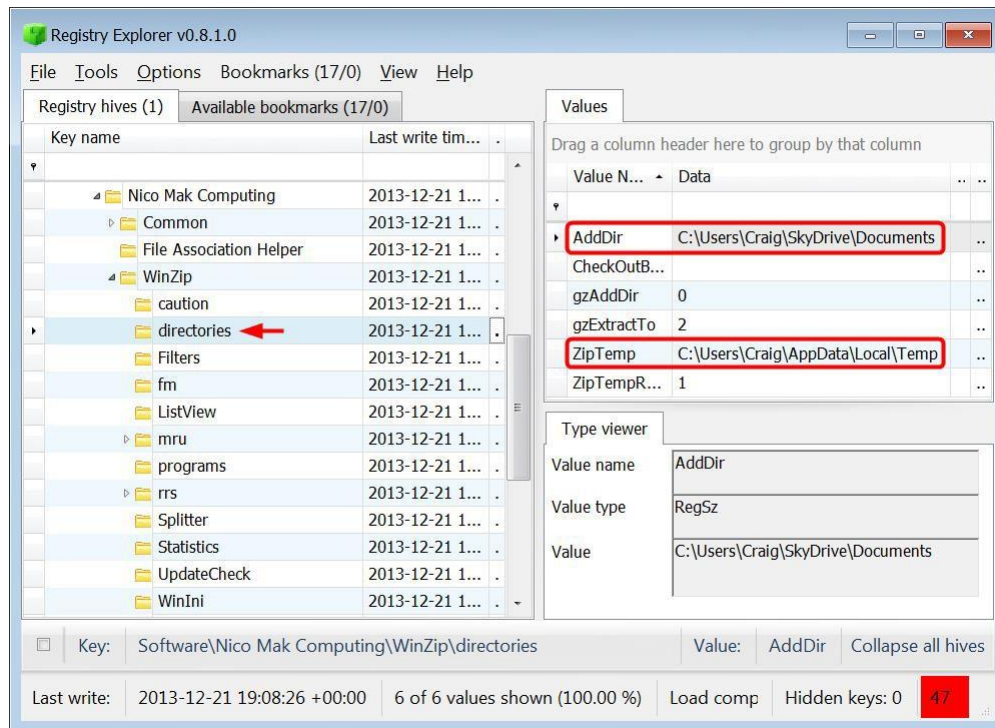
Figure 13-10 - AddDir and ZipTemp Values in Directories Subkey

The ZipTemp value shows you the location for temporary files. When a user opens a file in a ZIP using WinZIP, it will store the opened file in this temporary folder. The temporary folder location for this user is:

```
C:\Users\Craig\AppData\Local\Temp
```

However, if you look at this location in Autopsy, there aren't any files from WinZIP. You won't always find data in the temporary folder, because it's usually overwritten quickly. It's still a good idea to check it though.

The AddDir value shows you the last location a ZIP file was extracted to. In this case, it is:

```
C:\Users\Craig\SkyDrive\Documents
```

If you look at Craig's Skydrive, there are several coupons stored there. Now that you know this was the last location for a ZIP file to be extracted to, these coupons could have potentially been from the downloaded ZIP files. You also know that these coupons were downloaded from the Internet, because they have an ADS of 3.

Another piece of information in the NTUSER.DAT file is under the "mru\archives" subkey (see Figure 13-11).

Note: The abbreviation mru stands for "most recently used."
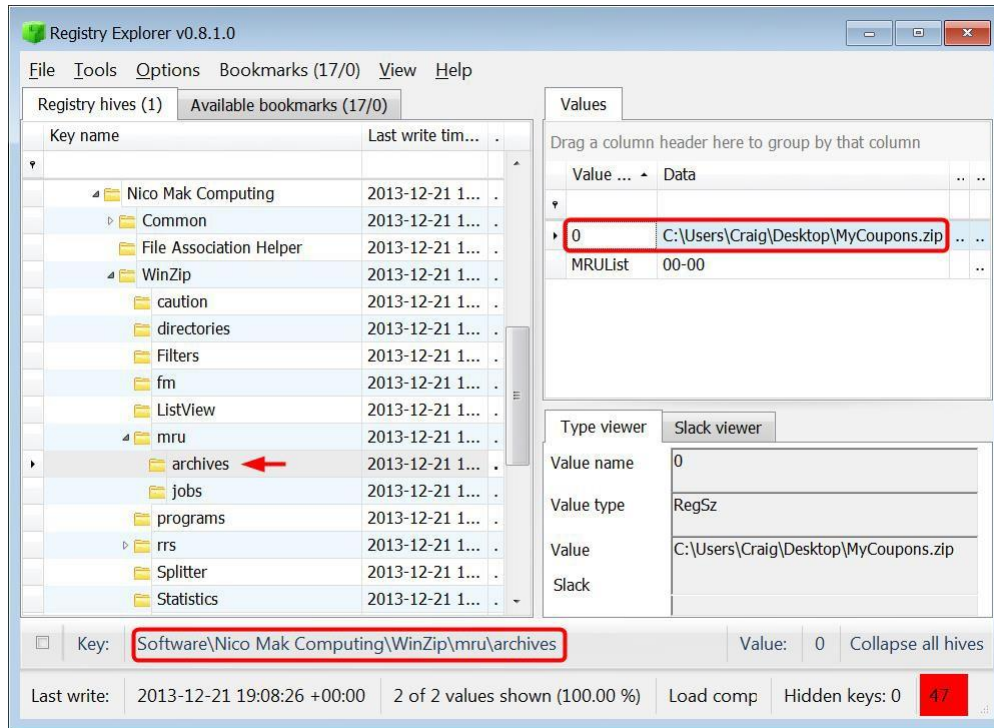
Figure 13-11 - ZIP File Created Using WinZIP

The values within this subkey will show what ZIP files were created using WinZIP. As you can see, there was only one ZIP file that Craig created using WinZIP, and it is the encrypted MyCoupons.zip on his desktop.

If you look at MyCoupons.zip on Craig's desktop, you will also notice that the Created and Modified times are the same. This is consistent with the ZIP file being created on Craig's computer.

WinRAR

WinRAR is another program used to compress and decompress ZIP and RAR files. Craig has a file called ALL COUPONS.rar located in his Downloads folder. Take a look at the following subkey in Craig's NTUSER.DAT file:

```
Software\WinRAR\ArcHistory
```
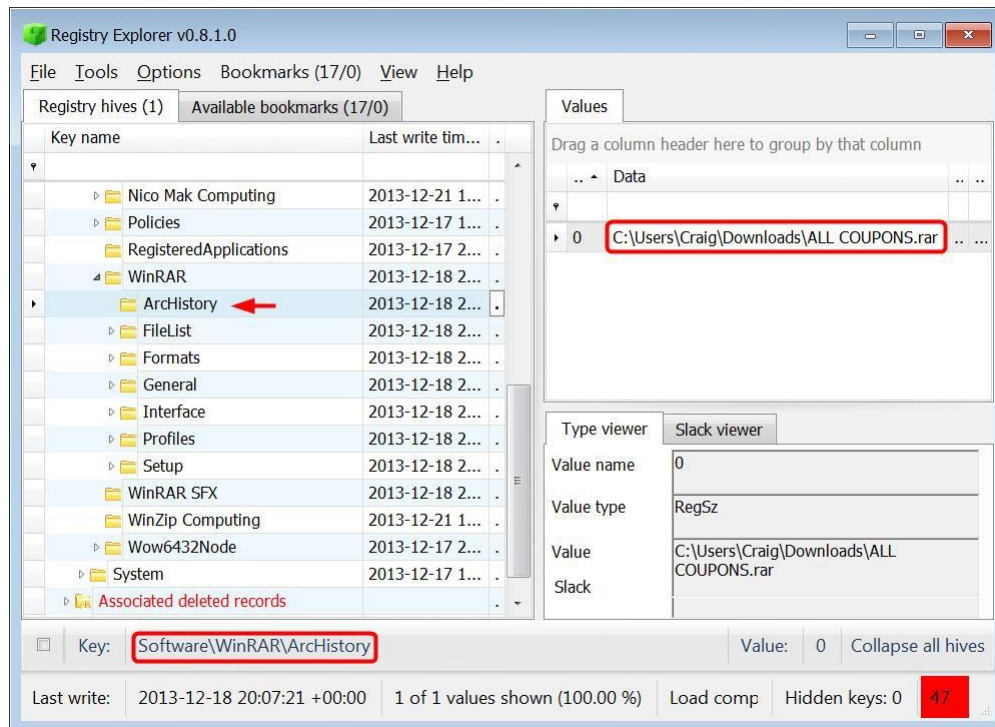

Figure 13-12 – ArcHistory Subkey Shows Files Opened with WinRAR

As you can see, WinRAR stores what files were opened in WinRAR under this subkey. If you wanted to see when the file was opened, you could look at Craig's Recent folder for any link files (see Figure 13-13).
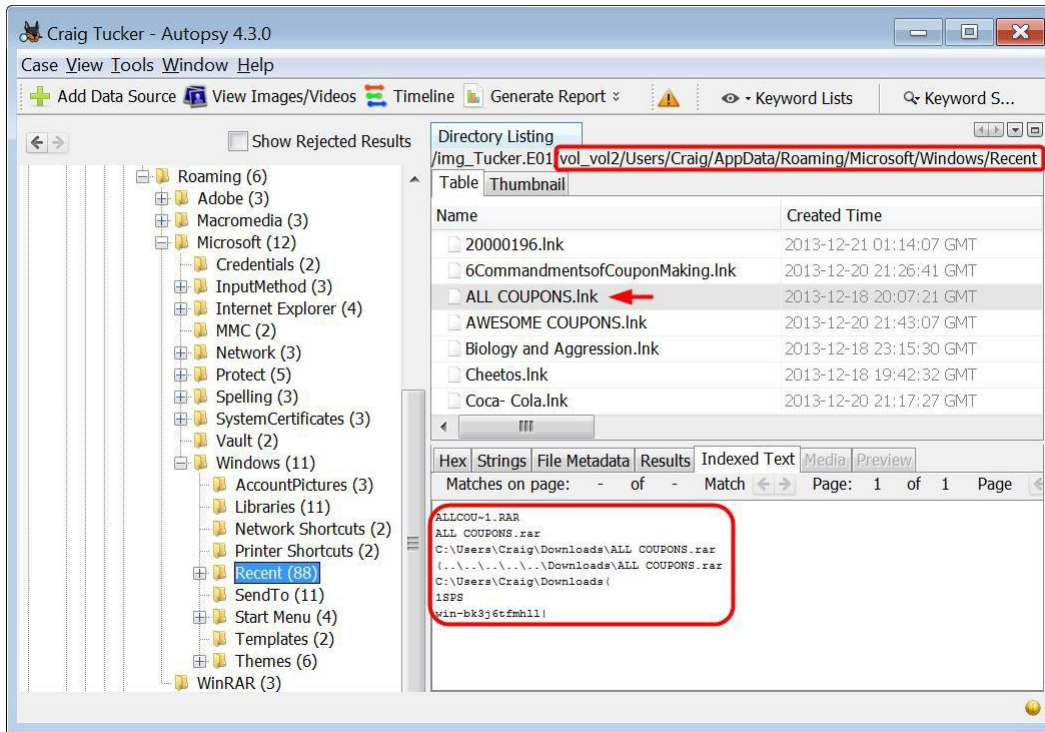
Figure 13-13 – Link File for ALL COUPONS.rar

As you can see, the Created time and the Modified time are the same on the link file, so ALL COUPONS.rar was only opened once on 12-18-2013 20:07:21 GMT.

Figure 13-14 – ALL COUPONS.rar Opened Once

Computer Forensics CCIC Training

Chapter 14: Legal

Bruce Pixley

May 2017 (Version 1)

14

Legal

Introduction

Once you start conducting forensic examinations of data, your role starts to fall into the category of an expert witness. As such, you need to be prepared to testify about your procedures and findings.

Whether you are simply preserving and collecting digital evidence or conducting the steps through analysis and reporting, you need to always do your job in a forensically-sound manner. If you do not, either you or another examiner may likely spend more time trying to explain to the court what you did and how that did not tamper or alter the original evidence.

If your case goes to trial, the court will have to determine if you are qualified to be an expert witness. The defense may try to challenge your designation as an expert by simply asking if you have a Ph.D. in computer science. However, an expert is not required to have a degree or major credentials. The court will determine if you are qualified based on your special knowledge, skills, training, or experience to provide testimony to aid the factfinder in matters that exceed common knowledge of ordinary people.

As you continue down the path of this field, keep track of your training and try to obtain credentials or certifications if you can. All of this will lead toward your qualifications to be designated by the court as an expert witness.

In federal court, the Daubert standard provides rules of evidence regarding the admissibility of expert testimony including scientific data. Digital evidence collected and analyzed using forensic software by an expert can be challenged.

What does this mean to you? The court will have to consider the admissibility of the digital evidence.

If the opposing side files a motion to suppress the evidence or challenge your skills based on the technology you used, the court will evaluate "whether the testimony's underlying reasoning or methodology is scientifically valid and properly can be applied to the facts at issue."

The court will consider factors such as:

- Whether the technique in question can be or has been tested;
- Whether it has been subjected to peer review and publication;
- The technique is known to have potential errors and there are maintenance standards controlling its operation;
- It is a widely accepted practice in the relevant scientific community.

As you go forward, you need to keep all of this in perspective as it affects how you do your job.

An excellent resource for legal issues related to digital evidence can be found on the U.S. Justice Department's website and is titled Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.

Expectation of Privacy

A search is considered to be constitutional if it does not violate a person's reasonable expectation of privacy.

A computer, storage media, and cell phone should be considered a "closed container" such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored on a computer if it would be prohibited from opening a closed container and examining its contents in the same situation.

Private Searches

Individuals who retain a reasonable expectation of privacy in the data stored on their computer may lose Fourth Amendment protections when they give their computer to a third party, such as a repair shop or a friend.

The Fourth Amendment is not violated when a search is conducted by a private individual acting on his own (not acting as an agent of the Government or with the participation or knowledge of any governmental official) and makes the results available to law enforcement.

Law enforcement can reenact the original private search without violating any reasonable expectation of privacy. However, law enforcement cannot exceed the scope of the original search. It is better for law enforcement to use the information learned from the private search as probable cause to get a warrant that will allow for a complete search.

Search Authority

Before you jump into any collection or search, you need to determine if you have the authority to do that.

If you are a government agent, then the Fourth Amendment applies to your actions. If a person is acting as an individual or on behalf of their company and not under the direction of the government, then the Fourth Amendment does not apply.

So what are the exceptions to a search warrant when it comes to digital evidence?

Consent

Law enforcement does not need a search warrant or even probable cause if the person with authority has voluntarily consented to the search. When using consent as an exception, you should consider the following factors:

- In the future, will you need to prove consent was given? How will you do that?
- When does a search exceed the scope of the consent?
- Who is the proper party to consent to a search?
- The consent may be revoked

Ideally, use a written consent form that states the scope of consent includes the consent to search computers and "other electronic storage devices."

When a third party gives consent to search a computer that consent may have some issues. For example, two people share a computer that is not password-protected. However, what if one person password-protected some files and the consenter does not know the password? You hit a crossroad, what should you do?

Parents can consent to searches of their children's computers when the children are under 18 years old. If the children are 18 or older, the parents may not have the authority to consent.

Computer searches by repairman prior to contact with law enforcement are private searches and do not violate the Fourth Amendment. Again, it is best practice for law enforcement to use the information revealed through a repairman's private search as a basis to secure a warrant for a full search of the computer.

Exigent Circumstances

When considering the use of exigent circumstances as an exception to the search warrant requirements, you need to consider the following:

- The degree of urgency
- The amount of time necessary to obtain a warrant
- Whether the evidence is about to be removed or destroyed
- The possibility of danger at the site
- Whether those in possession of the contraband know the police are on the trail
- The ready destructibility of the contraband

Just remember that the existence of exigent circumstances is tied to the facts of that particular case.

1. Can someone remotely issue a kill command to a cell phone? Yes. Could you seize a smartphone for the purpose of placing it in airplane mode? Probably, but conducting a search is another issue.
2. If an unlocked iPhone is allowed to enter a "locked screen" mode, will that prevent the investigator from accessing the data on the phone?
3. Can someone effectively lock their data on a computer that is using Microsoft Bitlocker?

Plain View

You are conducting a search of a computer for evidence of fraudulent documents and identification pursuant to a valid search warrant. During the examination, you see child pornography in "plain view." Do you continue to search for more child pornography or do you stop and seek a new search warrant?

At that point, stop your search for additional child pornography and obtain a new search warrant authorizing the search for that content.

The "plain view doctrine" does not authorize law enforcement to open and view the contents of a container that they are not otherwise authorized to open and review.

Probation and Parole

Individuals on probation, parole, or supervised release have a diminished expectation of privacy and may be subject to warrantless searches based on reasonable suspicion, or, potentially, without any particularized suspicion.

Search Incident to an Arrest

Pursuant to a lawful arrest, officers may conduct a "full search" of the arrested person, and a more limited search of his surrounding area, without a warrant. When it comes to computers, cell phones, or storage devices seized incident to an arrest, a complete forensic search often requires the data to be extracted and then searched using forensic software. While the devices may be seized, a search warrant needs to be obtained to conduct the search.

California Electronic Communications Privacy Act

Based on the passage of SB 178, four new Penal Code sections (1546, 1546.1, 1546.2 and 1546.4) became effective January 1, 2016, which is known as the California Electronic Communications Privacy Act (CalECPA).

The Act restricts government access to information contained in electronic form and mandates procedures for law enforcement to follow in order to obtain electronic evidence.

PC §1546 defines 12 terms used in the Act.

Computer Forensics CCIC Training

Chapter 15: Reporting and Timeline

Lauren Pixley, Cassidy Elwell, and James Poirier

March 2020 (Version 3)

15

Reporting and Timeline

Introduction

After you complete your analysis of the forensic image, you will need to create a timeline and a report. Since this is still an introduction to digital forensics, your report will be simple and you will only stick to the key points of Who, What, When, Where, Why, and How. You will also want to create a very simple timeline of only the important events that happened on the computer, such as an incriminating email being sent or a file of interest being opened. This chapter will use the Craig Tucker case as an example.

Report

For the CCIC Event, you are expected to create a presentation (PowerPoint, Prezi, etc) that discusses Who, What, When, Where, and How. When you answer these questions, you will want to support your answer with as much evidence as possible. You can back up your answer with emails, Internet searches, files opened, or anything else of interest that relates to your response. For your presentation, you will want to have your title slide with the case name and each team member name.

Figure 15-1 – Title Slide with Case Name and Team Member Names

Your next slides should focus on the Who part of the report. When writing your answers on who the suspect is and who they were communicating with, you can easily go beyond just the simple points made below for the Craig Tucker case. Some cases you might find pictures of the suspect, personal documents with their information, or see them logging into personal accounts online.

Who was the suspect?

1. You know based on the scenario given at the beginning that the main suspect was Craig Tucker.
2. After searching through the Windows Registry, you determined the only user account was named Craig.
3. After going through the Windows 8 Mail App, you found emails that were sent and received by Craig Tucker under the email address "coupon-king@outlook.com".
4. After looking at the Google Chrome history and Windows 8 mail, you found Facebook accounts for Craig Tucker.
5. After reviewing the Skype chat logs, you saw chats to and from Craig Tucker.

Reporting on who was using the computer is important, because later you want to be able to prove that the suspect was the actual one behind the keyboard. You will also want to report who the suspect was talking to, because you may need to make recommendations to go after other accomplices. Your second slide after your title slide should focus on who the suspect was.

Figure 15-2 – Slide on Suspect

After the second slide, you will want to include a slide on who the suspect was communicating with. This can include people he simply talked to or actual accomplices to a crime. Make sure to support your findings and show how the suspect knows the person if possible. You will also want to report who the suspect was talking to, because you may need to make recommendations to go after other accomplices.

Who did the suspect talk to or work with?

1. Craig sent and received emails from Stan Marsh, Kyle Broflovski, and Kenny McCormick about creating coupons. They also traded email attachments of coupons and guides on how to make them.
2. Craig talked to Kenny McCormick through Skype chat about coupons.
3. Craig sent and received emails from Stan Marsh about underage pictures.

Figure 15-3 – Slide on Witnesses and Accomplices

Next, focus on the What section of your report. For this section, you want to include what crimes the suspect committed or what they were planning on doing. You can support this through emails, documents, guides, chat, or anything else that shows they intentionally did something or planned something (see Figure 15-4). The What section can be put into one slide or multiple ones if necessary.

What did the suspect do? What was the suspect planning on doing?

1. Craig had accessed fraudulent coupons stored in his documents subfolders.
2. Craig had some images depicting child pornography in the recycle bin, but had other child pornography images stored in other locations.
3. Craig potentially has other child pornography and fraudulent coupons stored on external storage devices.
4. Craig sent and received fraudulent retail coupons.
5. Craig intentionally searched for and downloaded fraudulent retail coupons from the Internet.
6. Craig modified and produced fraudulent retail coupons, which were subsequently used to commit theft against a retail store.
7. Craig sent and received images depicting child pornography.
8. Craig talked with others about creating and using fraudulent coupons at a retail store.
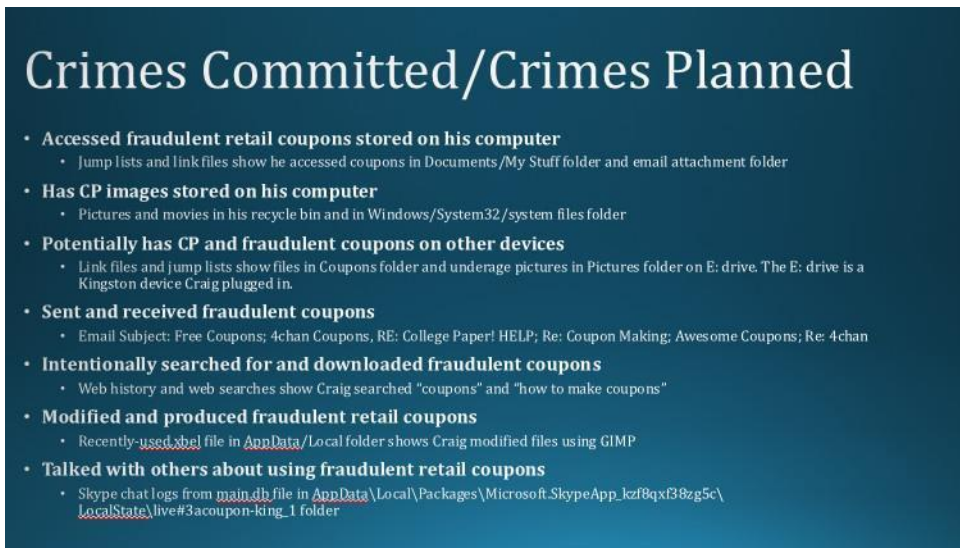
Figure 15-4 – Slide on Crimes Committed or Crimes Planned

After covering the What section, you will want to cover the How section. This ties together with the What part because you need to not only answer what the suspect did or planned on doing, but also how they did something or planned on doing something. You can include what software they used to accomplish something, how they used external drives to store and access data, or documents and chat that shows how they were going to commit a crime.

How did the suspect do the crime? How was the suspect planning on committing a crime?

1. Craig plugged in an external drive to access potential CP and fraudulent coupons.
2. Craig used the Windows 8 Mail App to send and receive emails with CP and fraudulent coupon attachments.
3. Craig used Google Chrome to search for and download fraudulent coupons.
4. Craig used GIMP to modify and create fraudulent coupons.
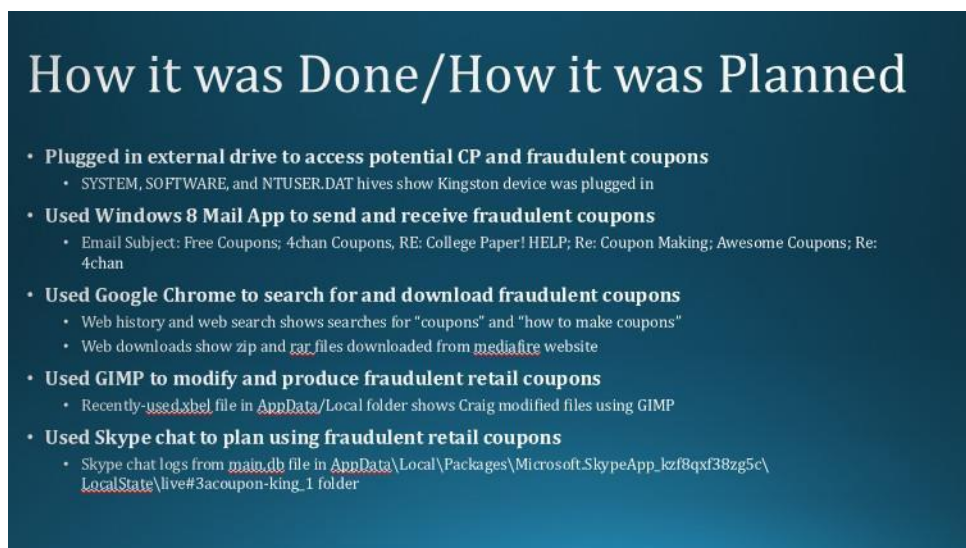5. Craig used Skype chat to plan with Kenny on using fraudulent coupons at Walmart.

Figure 15-5 – Slide on How Crime was Committed or How Crime was Planned

The next part of the report is Where. The Tucker case does not really have that much location information. You know that he was caught at Walmart using fraudulent coupons. He also chatted with Kenny McCormick about going to Walmart to use fraudulent coupons.
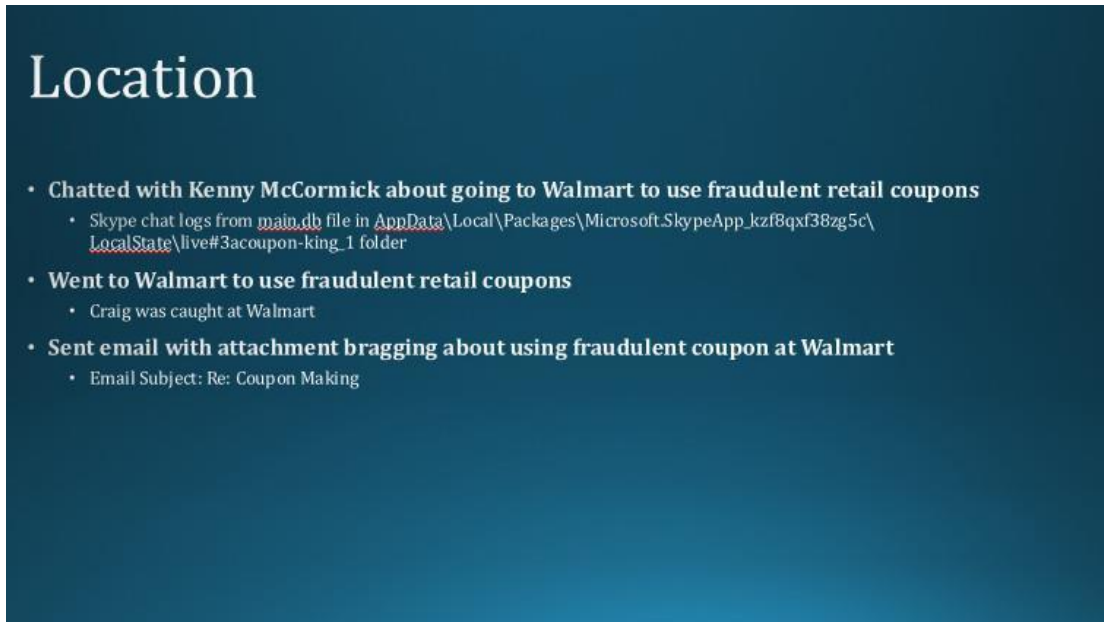

Figure 15-6 Slide on Location of Crime or Planned Location of Crime

Some other cases you may be able to show more information on where the suspect did something or where they were planning on doing something. You can support your answer by providing time stamps, emails, chats, Internet history, or any other activity related to locations.

One slide you could potentially include is based on Why. You are not the suspect, so you cannot truly know why the person might have done what they did or planned to do something. However, you can speculate based on the evidence you found, such as needing money, wanting revenge, etc. In the Tucker case, there really is not a reason for why Tucker used fraudulent coupons, other than possibly wanting to save money, so I am not going to include a why section for this case.

Timeline

After working on the Who, What, How, and Where sections, you will probably want to include a section on When for your report. You will want to show when the suspect did certain things or when they planned on doing something. The best way to achieve this is by creating a timeline. Timeline analysis can usually become very complicated when you actually go into all the details about what was happening on the computer. Since this is still an introduction to digital forensics, you are only going to create a very simple timeline.

For this project, you will want to use the Office Timeline tool. You can download the 14-day free trial at the following website:

```
https://www.officetimeline.com/14-days-trial
```

Note: You only need to enter an email address to get the 14-day free trial. Once they send you the Plus Edition product key to the email address, simply open PowerPoint and click the Activate button under the Office Timeline Free tab. From there, you just need to paste the product key and click the Activate button.

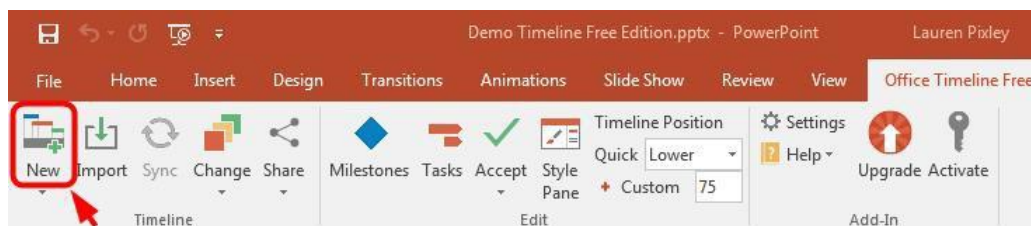Once you have Office Timeline downloaded and installed, open Office Timeline and click the New button.

Figure 15-7 – Click New Button on Office Timeline

When the Create New Timeline window opens, select the Metro timeline. Then, click the Next arrow in the bottom right corner.
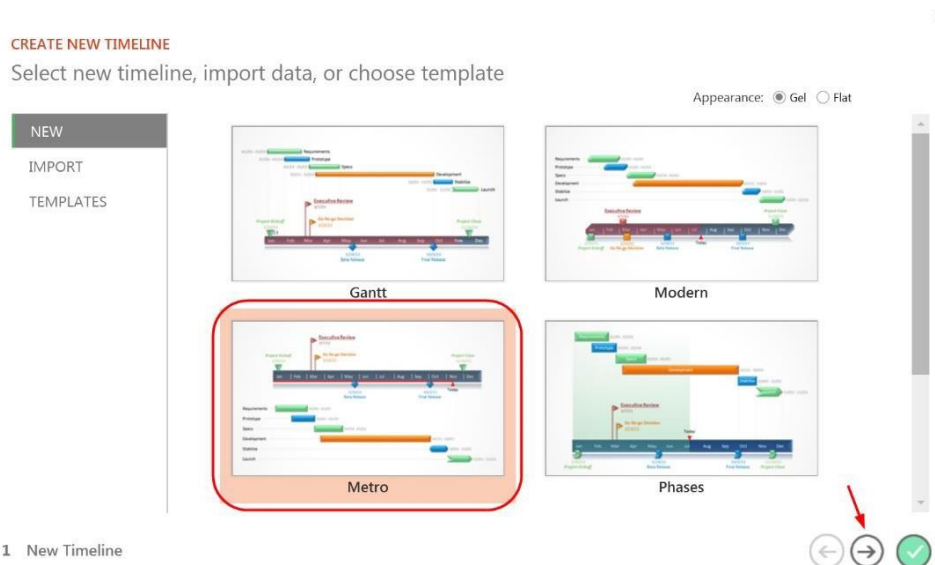

Figure 15-8 – Select Metro and Click Next Arrow

On the next window, you will be prompted to enter the events and dates. You will also need to the click the Clock button in the top right corner to add time stamps to each event. Use the Plus button in the top right corner to continue to add more events. You can set different colors and shapes based on the types of events. You may also want to check the Below box for certain events so the event text stays within the bounds of the PowerPoint slide.

Ultimately it is up to you what events you want to include in your timeline. You may want to show when certain Internet, file, email, or USB activity occurred. When creating your timeline, you may want to either create a separate slide for each day or keep your timeline to only specific simple events. This will help prevent the timeline from looking cluttered or confusing. For the Tucker case, I split the events that occurred on the 18th to just one slide. Once you add all the events you want, click the Finish button in the bottom right corner.
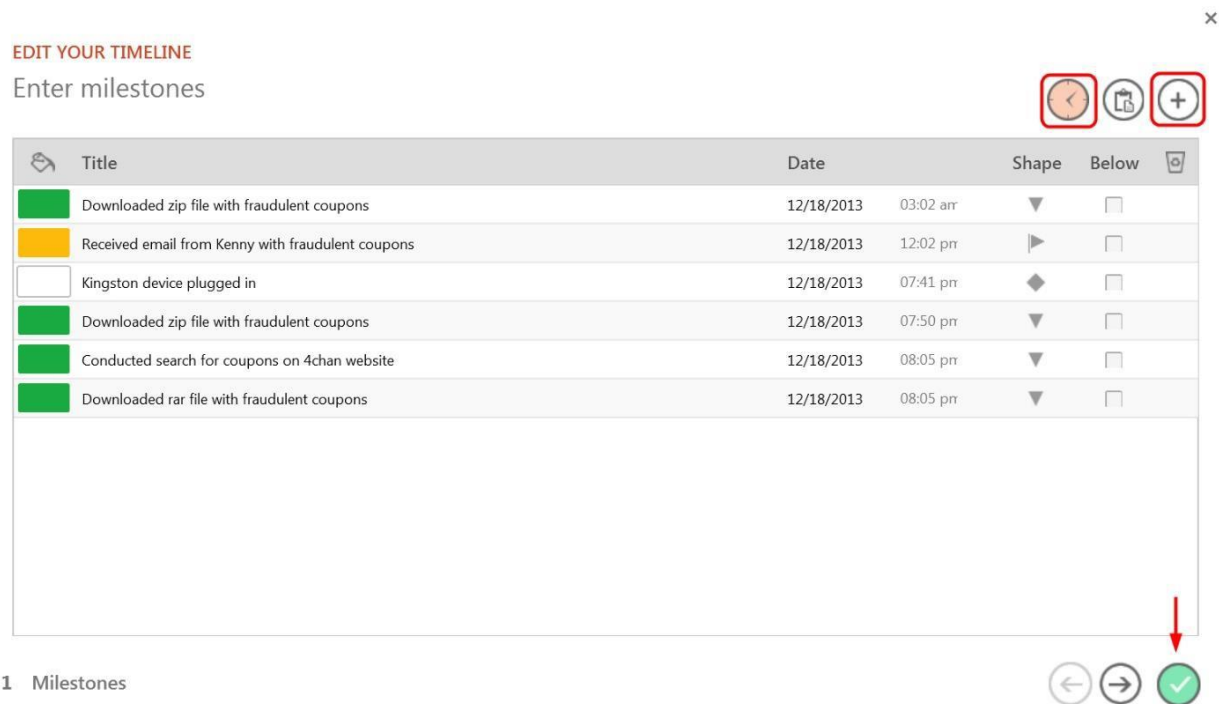

Figure 15-9 – Add Events, Dates, and Times and Click Finish

Since most of your events are broken down by the hour, you will want to change the timeline scale. To do this, click on the Style Pane button under the Office Timeline+ tab. Then, click on the Timeline scale in the main slide. The right pane of PowerPoint will show a button called Timeline Scale. Click on it and then select Hours/Minutes (see Figure 15-10).
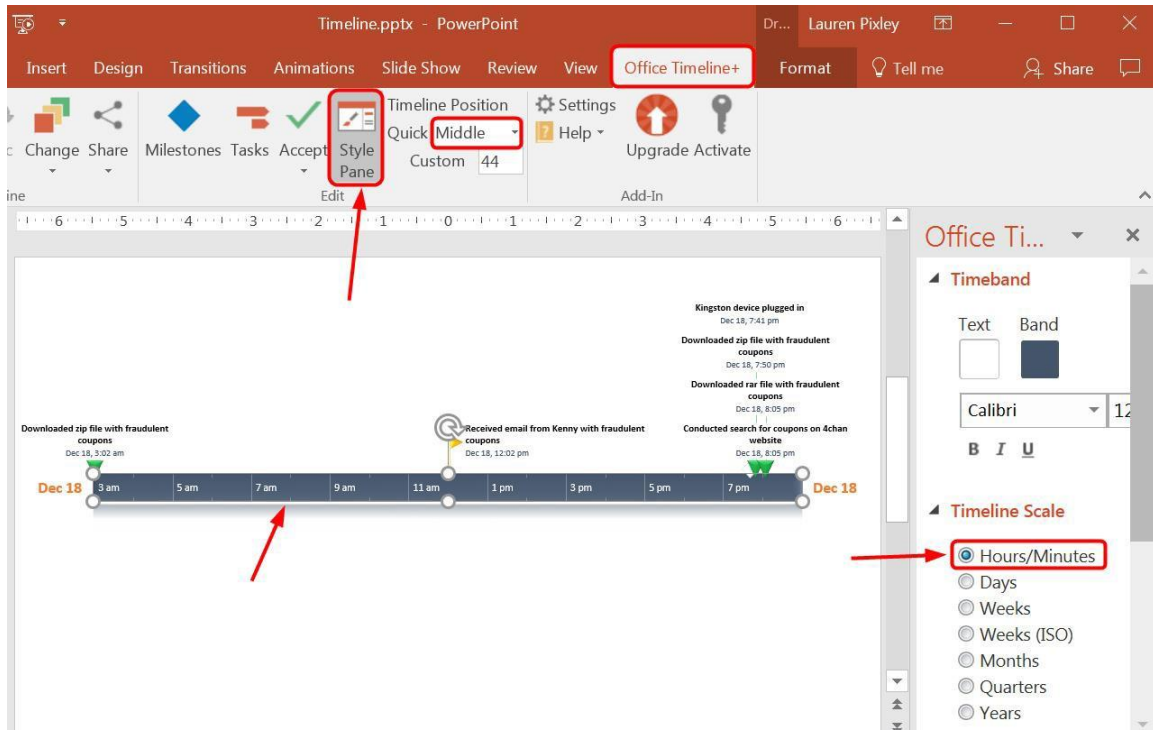
Figure 15-10 – Click Style Pane Button, Select Timeline Scale in Slide, and Choose Hours/Minutes under Timeline Scale

Note: You can also change where the timeline scale is by clicking the drop-down menu in the top bar called Timeline Position. The Middle position may work the best because you can then choose to have some events displayed above the timeline and some below.

After creating a timeline for one set of events, you can create another timeline on a different slide. This may help separate the days and keep your timeline from getting cluttered. However, it is ultimately up to you to choose what events you want to show in your timeline and how you want to report and present it.
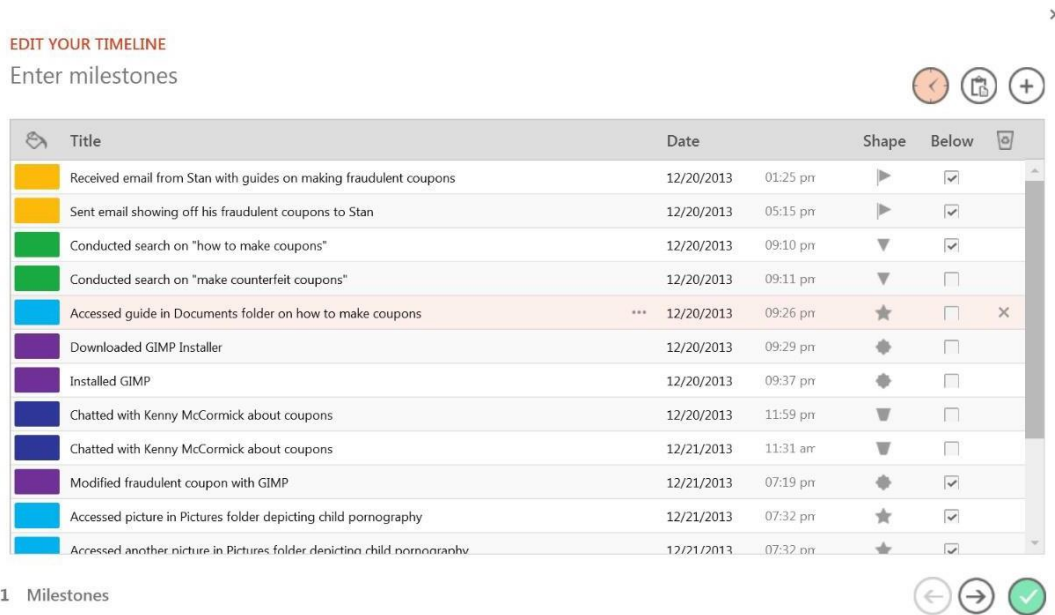

Figure 15-11 – Timeline with More Events on Second Slide

Depending on what case you are working on, you may want to show specific events that help support your Who, What, When, Where, and How points you previously made in your slides. For example, on the Tucker crime slide I showed a bullet point on how Tucker used GIMP to modify and produce fraudulent retail coupons. I then included in my timeline when Tucker downloaded and installed GIMP, when he accessed guides on how to make coupons, and when he modified a fraudulent coupon with GIMP.

If the case you are working on has a suspect planning to do something on a certain date, you may want to include that in your timeline as well. Again, it is up to you to decide how to best show your work and support your argument.
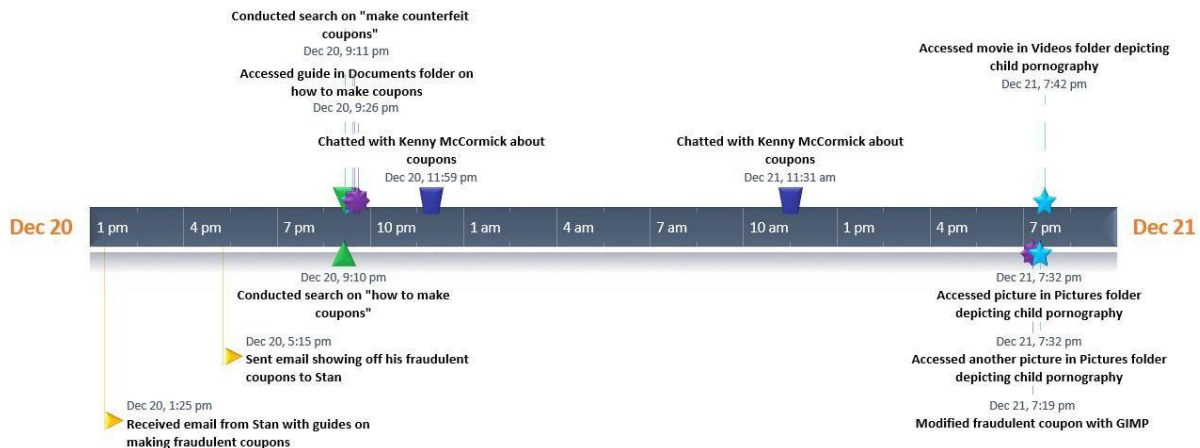

Figure 15-12 – Timeline of Events

After creating your timeline slides, you can also do a slide that just lists some events that you want to discuss further. For example, if the suspect planned on doing something, you may want to include a separate slide that discusses your findings further. It is up to you how you want to present all your findings.

One last slide you should include is a recommendation slide for the event. As an examiner, you may not always be asked to make recommendations, but for this event you will need to come up with recommendations based on your findings. Some possible recommendations include other accomplices that need to be looked into or where a suspect might be if they are on the run. For the Tucker case, the only real recommendation you could make is to look into Stan, Kyle, and Kenny because they traded coupons and underage pictures with Craig (see Figure 5-13).
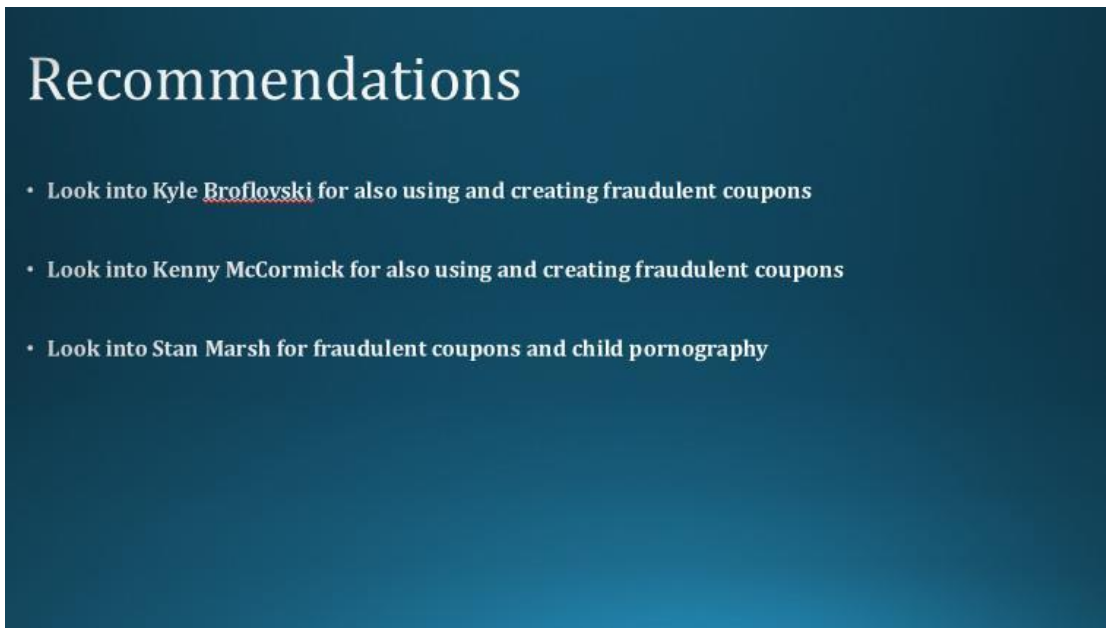
Figure 15-13 Slide with Recommendations Based on Findings